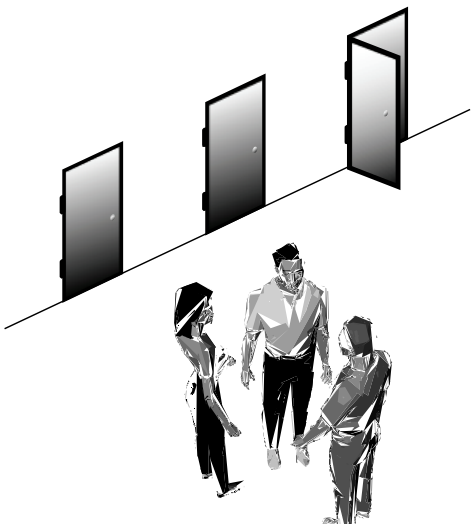
SIEMENS



SiPass Entro

Installation

MP6.5 SP1

Building Technologies

Fire Safety & Security Products

Technical specifications and availability subject to change without notice.

© 2010 Copyright Siemens Switzerland Ltd

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

Table of contents

1 About this document 8

2 Safety 9

2.1 Target group 9

3 Description of equipment 10

3.1 Software description 10
3.1.1 Software applications 10
3.1.2 Software windows 11

3.2 System overview 12

3.3 System capacity and limits 13

3.4 System components 14
3.4.1 Enrolment reader kit 18

3.5 Small applications – without LAN 18

3.6 Larger applications – with/without LAN 19

3.7 Communication with PC 22
3.7.1 Local Area Network 22
3.7.2 RS232 23
3.7.3 Modem 23

3.8 Connect more than one PC 24
3.8.1 Multi-user database 24
3.8.2 Microsoft Terminal server 2008 25

3.9 Global communication between several SR35i 25
3.9.1 RS485 25
3.9.2 Ethernet with TCP/IP 25
3.9.3 Example of SR35i with RS485 26
3.9.4 Example of SR35i used in Local Area Networks 27
3.9.5 Example of SR35i using Internet 28

3.10 Wireless communication 29

3.11 Reservation 29
3.11.1 Integrated Web server 30
3.11.2 How the Reservation system is installed 31

3.12 Integrate CCTV system 31

3.13 Integrating with external applications (BAPSI) 32
3.13.1 General 32
3.13.2 What is BAPSI used for? 32
3.13.3 Field applications 32
3.13.3.1 Application example - External Reservation system 33

4 System requirements 34

4.1 Recommended system cables 35

4.2 Cables 36
4.2.1 Cable for power supply 36
4.2.2 Cable for RS485 36
4.2.3 Cable for network (TCP/IP) 37
4.2.4 Cable to PC 37
4.2.5 Earthing and screening for RS485 37

5 Power supplies 38

5.1 Central DC power supply 38
5.2 Local DC Power Supply 39
5.3 Voltage drop 40
5.4 Example of a typical power supply section 41
5.5 Several DC power supplies in the same cable section 41

6 Special installations 42
6.1 Anti-pass back using BCLINK readers 42
6.2 Anti-pass back using Clock&Data and Wiegand readers 43
6.3 Intrusion Alarm Zones with DC22 44
6.4 Connecting Alarm Status Feedback in DC22 (ASF) 45

7 Quick start guide 46

8 Connect the PCs or an online printer 47
8.1 Connect PC via Local Area Network 47
8.2 Connect PC with direct cable (RS232) 48
8.3 Connect an on-line printer (RS232) 48

9 Prepare any network resources 49
9.1 Background 49
9.2 Subnet agent (SR35i) 50
9.3 Router setup 51
9.4 DynDNS 51
9.4.1 Configuring of DynDNS.org 52
9.5 Firewall 52
9.6 Example with router 53
9.7 Apartment building – example 54

10 Installing the software 55
10.1 Creating a basic database and connection 55
10.1.1 Automatic detection of units 57
10.2 Multi-user environment (more PCs) 58

11 Installing modem based systems 59
11.1 Configuring a system equipped with TD36 modem (recommended) 60
11.2 Configuring a system equipped with a custom modem 60
11.3 Configuring the modem based system on site 60
11.4 Mount and configure the modem 62
11.5 Transferring the new system's information to the central PC 63

12 Installing the CF8 flash memory card 64

13 Install DVRs 65
13.1 Prerequisites 65
13.2 DVR connection 66
13.3 How to control recordings? 67
13.4 Camera settings 67
13.5 SISTORE™ MX 68
13.5.1 MX Parameters 69

13.5.2 MX Live Viewer software 69
13.5.3 Additional considerations for the MX 69
13.6 SISTORE™ AX 70
13.6.1 General 70
13.6.2 AX9 and AX16 70
13.6.3 AX4 and AX Lite 70
13.6.4 AX Parameters 71
13.6.5 Additional considerations for the AX 72
13.6.6 AX Live Viewer software 72
13.7 SISTORE™ CX 72
13.7.1 General 72
13.7.2 CX Parameters 73
13.7.3 CX Live Viewer software 73
13.7.4 Additional considerations for the CX 73

14 Before configuring the system 74
14.1 Check the communication circuits 74
14.2 Check the power supply 74

15 Checklist 75

16 Start the software 76
16.1 Indicators for communication status 77

17 Set time and date 79

18 Advanced system clock management 80

19 Personalize Entro settings 81
19.1 Card reader parameters 81
19.2 Personal code without card 81
19.3 Changing red LED function on readers 82
19.4 Duress code on/off 82

20 Configure names for segment controllers 83
20.1 Create multiple SR35i for TCP/IP communication 83
20.2 Create multiple SR35i for combined TCP/IP & RS485 communication 84
20.3 Create multiple SR35i for only RS485 communication 85

21 SR35i Configuring 86
21.1 Decide on network settings for SR35i 87
21.2 Customize the database for DHCP 89
21.3 Prepare the SR35i component for DHCP 90

22 Configure names and functions for doors 91

23 Configure IOR6 relay controller 92

23.1 Door lock monitor - output 92
23.2 Common alarm – output 93
23.3 Configure IOR6 for time control 93
23.4 Power failure warning - input 94
23.5 Emergency opening – input 94
23.6 Exit button - input 94
23.7 Configure IOR6 for Reservation system 95
23.8 Lift Control with IOR6 95

24 Configure Intrusion Alarm zones 97
24.1 Decide on security levels for alarm control 99

25 Configure other type of zones 100
25.1 Anti-pass back/Roll call 100
25.2 Entrance limitation 101
25.3 Interlock zone 102
25.3.1 Example Interlock 102

26 Configure for reservation 104
26.1 Setup zones for reservation object 104
26.2 Random allocation or NOT of similar reservation objects 105
26.3 Alarm control in a reservation object 105
26.4 Time schedules 106
26.5 Reservation object 107
26.6 Enter public holidays and holiday periods in Reservation 108
26.7 Decide on reservation authorities for access groups 108
26.8 Give persons reservation authorities 109
26.9 Flexible reservation in same interval 110
26.10 Show reservation information to the user 110
26.11 Service mode 110
26.12 Setup for debit function 111
26.13 Configure for e-mail confirmations 111
26.13.1 Prerequisites for confirmations 112
26.13.2 Editing text in the confirmations 113
26.13.3 Example of confirmation 113
26.13.3.1 Table of e-mail fields in reservation confirmations 114
26.13.3.2 Special e-mail fields 114

27 Maintenance 115
27.1 Expanding and modifying the system 115
27.2 RS485 115
27.3 Networking 115
27.4 Software update in existing system 116
27.5 Installing an additional – or replacing a PC 117
27.5.1 Prepare the database in the existing PC 117
27.5.2 Configure the additional – or replaced PC 118

27.6 Installing an additional – or replacing a SR35i 118
27.7 Installing more readers 119
27.8 SR35i firmware control 120
27.9 Saving/restoring database on CF8 120
27.10 Door controller firmware control 121
27.11 Printout of system configuration 121
27.12 Migrating from a Entro Lite system 121
27.13 Uninstalling Entro 121

28 FAQ 122
28.1 Advanced information about LAN 122
28.2 What redundancy is there in the system? 124

29 Important information form 126

30 Index 127

1 About this document

This document contains information on the installation of the product.

Other related documents are:

- SiPass Entro Project design manual which describes important concepts.
- SiPass Entro User manual which describes the operation of the software.

For the installation of the hardware components please refer to the hardware manuals of the components.

Note - if you have been using earlier versions of SiPass Entro documentation, you will now find information about some software configuring details in this Installation manual (instead of the User manual).

2 Safety

2.1 Target group

Target readers	Qualification	Activity	Condition of the product
Installer	Technical training for electrical installations.	Installs the product, individual components of the product or replacement parts.	Components of the product are not yet installed or need to be replaced or modified.
Operational start-up personnel	Technical training for electrical installations. Training on the product is recommended.	Puts the product into operation for the first time, or changes the existing configuration.	The product is installed but not yet configured, or the existing configuration is to be changed.
Service personnel	Technical training for electrical installations.	Checks the product at regular intervals to ensure that it is in good working order and performs service work.	Product already in use and requiring servicing.

3 Description of equipment

3.1 Software description

3.1.1 Software applications

The SiPass Entro software consists of three applications:

Installer

This application is used for setup of the hardware. Install PC, Controllers and door monitor contact and alarm zones.

Entro

This application is used for configuring and managing access groups and persons (cardholders). It can be treated as main part of the software, because it is used for daily operations.

The following functions are integrated in the Entro:

- Access control
  Add Cardholder, choose and configure Caretakers, create Access Groups, create Time Schedules, Zones (anti-pass-back zones, roll call zones, entrance limitation zones
- Card printing (badge printing)
  Create your own card design and print it on an industry standard cards.
- Video Surveillance (CCTV) integration
  The SiPass Entro system can be used in combination with a Siemens CCTV system. A connection can be done from the SiPass Entro software directly to install and maintain the CCTV system (e. g. DVRs and cameras)
- Intrusion alarm system control
  A common application for the SiPass Entro is, beside access control, to control an external intrusion alarm system by means of an access card.
- Reservation function
  The System Administrator sets which objects (such as card readers/doors) are to be included and chooses the relevant reservation time schedules.
  The users wanting to reserve times can use an ordinary web-browser (such as Internet Explorer). Alternatively use his/her card in a reservation terminal (InfoPoint IP811) – depending on how the system is configured.
- Printouts

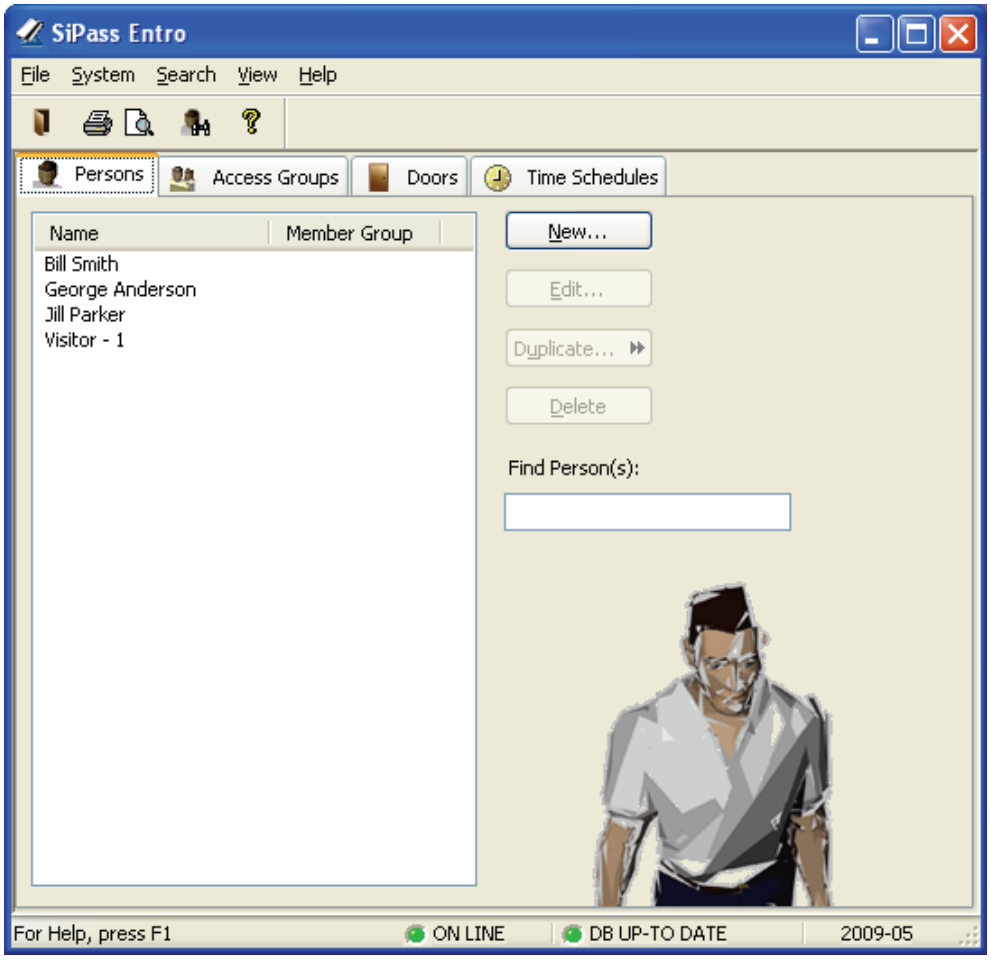
Door Monitor

This application is used to display event logs, door status and video sequences. It can be also used for unlocking doors via the PC.

3.1.2 Software windows

Entro starting window

When the Entro application is started the following windows is displayed (showing the list of persons):



Entro start window

Shortcuts

There are two shortcuts sometimes available in the software, to help creating, editing or deleting information. They appear e g in the Access group properties and in the Person's properties.

Shortcut to Time schedule

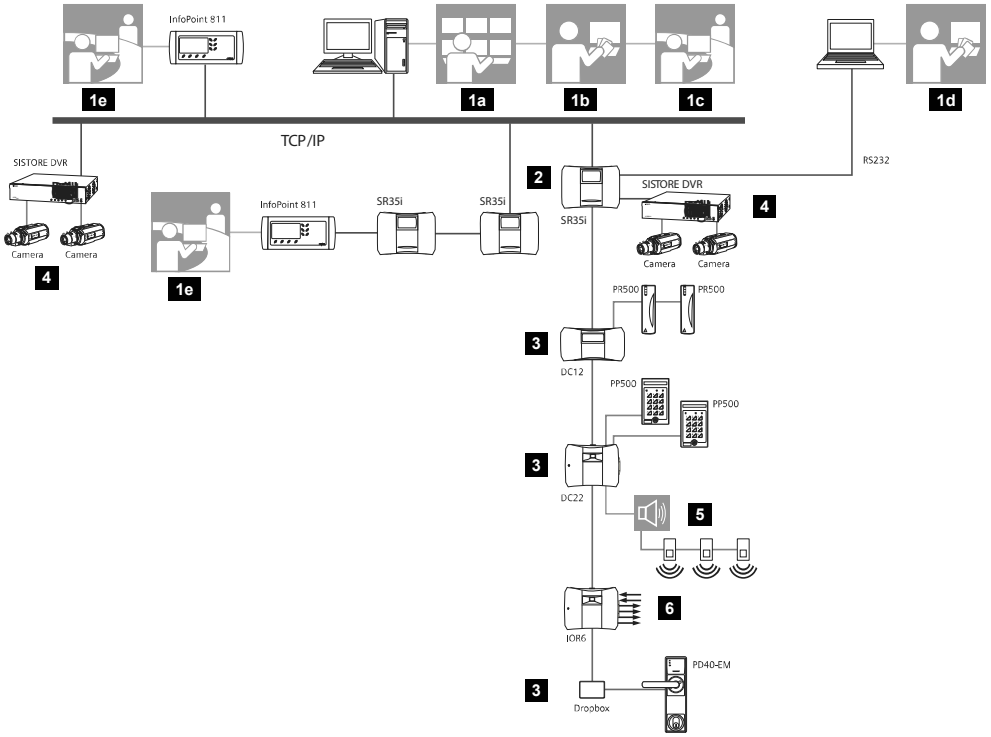
Shortcut to Access groups

E. g. when you create a new person, click on the shortcut **Access group** if you have not yet created a suitable one. In the same manner you can click further to **Time schedule** if you want to create or edit a time schedule. In all cases you will come back to the previous step when you exit the menus.

3.2 System overview

The system below is shown on three levels:

- PC (with software) to send/receive information to/from the system via direct cable or network. The InfoPoint IP811 terminal is used for reservation functions.
- SR35i controllers hold information and make decisions as to the access granted at the doors.
- Door environments where door controllers, readers, keypads etc. are installed together with electrical locks.



Different levels in the system.

1a	PC – Security Controller
1b	PC – System Administration
1c	PC – Visitor Management
1d	Local PC – System Administration
1e	Reservation Management
2	Controllers
3	Doors
4	Video surveillance system connection (TCP/IP)
5	Intrusion alarm control (relay output)
6	Control inputs and outputs

3.3 System capacity and limits

SiPass Entro software

Software for control of up to 10 000 systems, each capable of managing up to:

- 512 wired doors and 512 wireless doors (RF) in up to sixteen controllers
- 40 000 cards
- 240 time schedules
- 480 access groups
- 240 zones (alarm, anti pass back, roll call, interlock and entrance limitation zones)
- 16 system users in 4 levels + installer level
- 14 holidays, 7 half days and 4 holiday periods in each time schedule

Reservation functions

- 64 reservation objects (machine groups)
- Maximum of 30 doors and/or IOR6 relays in each reservation object
- 32 time schedules with 24 intervals in each
- Flexible interval reservation
- Maximum number of reservations is 6100

Video Surveillance (CCTV) integration

- Maximum 16 DVR - one DVR per SR35i/SR34i
- Maximum 128 cameras

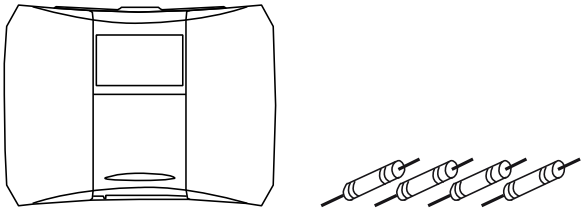
Card printing

- Multiple card and/or receipt template design
- Bulk printing of cards

3.4 System components

There are different products included in the SiPass Entro range of components.

- **SR35i Segment controllers**. Up to 16 segment controllers can be connected to the PC in a “daisy chain” configuration. Each segment controller can control 4 wired + 4 wireless, 8+8, 16+16 or 32+32 doors. The information you program in the PC is stored in all segment controllers. This has the advantage of being able to use the PC for other purposes or shut it off when it is not configuring or monitoring SiPass Entro.



Each segment controller is delivered with 4 termination resistors (120 Ω).

The Segment Controller is available in four different capacities which indicate how many doors it can manage:

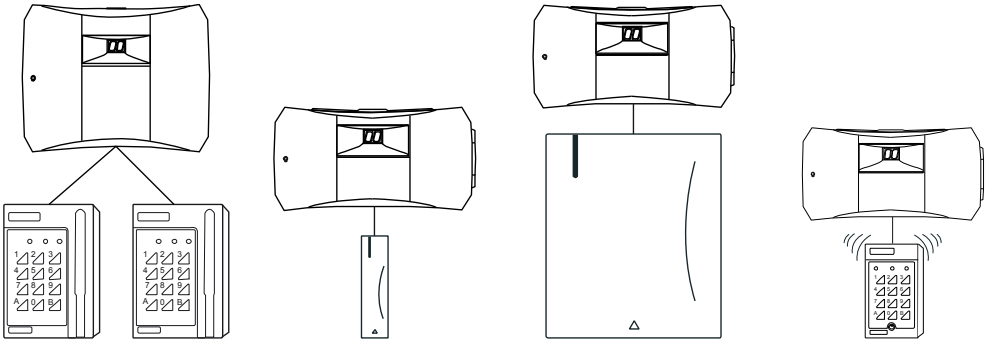
SR35i/4	Controls max four doors
SR35i/8	Controls max eight doors
SR35i/16	Controls max 16 doors
SR35i/32	Controls max 32 doors

It is possible to upgrade and extend the capacity gradually. This eases future expansion.

The SR35i communicates on two levels (global and local bus). It gives many choices of how to specify SiPass Entro. Properties with several floors can include a SR35i on each floor which can handle a couple of doors each.

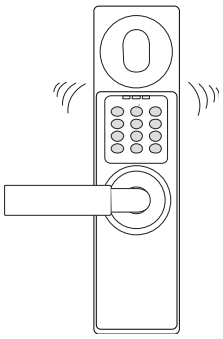
The most important is the SR35i Segment Controller which contains all data about the site. Even the User name and password for the PC software package is included.

- **Door controllers with remote card readers**. The door controllers are connected to the segment controllers. A door controller controls one door where one or two (in/out) remote card readers can be installed. This combination (split installation) is designed for external doors or other doors with higher requirements on function and security, e.g. alarm by-pass and door control.

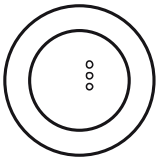


1.	DC22 with Magnetic card or proximity readers.
2.	DC12 with Proximity reader.
3.	DC12 with Hands-Free reader.
4.	DC12 with proximity reader (PP500) with PIN pad in small housing

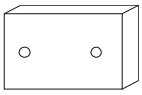
- **Proximity Codoor PD30-EM/PD40-EM.** Electromechanical unit equipped with a proximity reader for EM technology. Connects to the Segment controllers. PD30-EM fits primary Scandinavian lock cases and PD40-EM the Euro standard.
- **Radio link RF Codoor RF30-EM**. Communicates wireless to the Segment controllers directly or via RF9 routers.



- **RF9**. Wireless router used for amplifying and routing the RF signal.

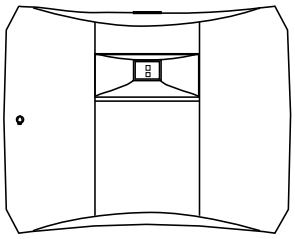


- **Door controllers without remote terminals**. In some cases there is a need for monitoring or opening a door by time schedule. The DC01 can be used as a timer controlled relay or monitoring unit.



Door controller DC01

- **Relay controller.** To control e g a lift the IOR6 can be used. Any reader can control which relays to activate. The IOR6 can be used in reservation applications. Version 5 onwards also offers functions like Common alarm, Lift control, emergency opening and power failure monitoring.

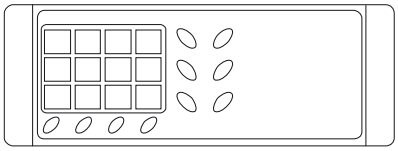


Relay controller IOR6

- **CF8**. If Reservation is to be used a CF8 memory card must be installed in one of the SR35i segment controllers.

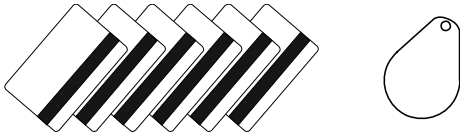
CF8 Memory card

- **Reservation terminal**. An InfoPoint IP811 can be used in a reservation system enabling reservation local to the object. Includes an integrated card reader function for identification.

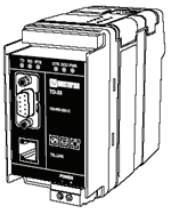


InfoPoint IP811

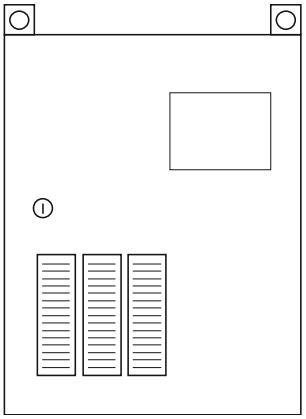
- **Cards**. Every person would use either a card or proximity tag.



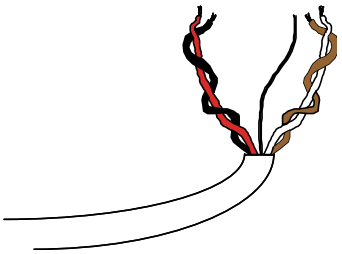
- **Modem.** If multiple SiPass Entro systems make up the installation, a modem may be connected for communication between the systems and the central PC.



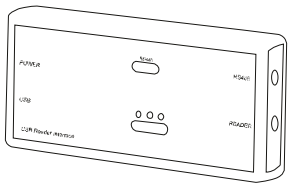
- **Battery backup**. One or more battery backup power supplies are recommended for the system's power.



- **Cables**.

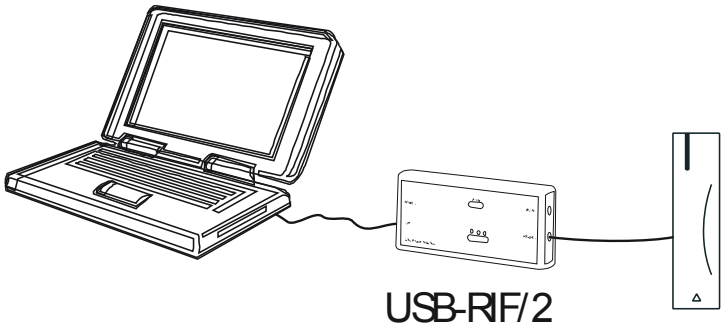


- **USB-RIF/2** – used for enrolment and log on functions



USB to Reader interface converter

3.4.1 Enrolment reader kit



USB-RIF/2 to PC.

In SiPass Entro, an enrolment reader can be connected directly to a PC via the reader interface USB-RIF/2. It can be used for:

- Login of cards
- Login to system software with card.
- Fast search of card holders.

USB-RIF/2 connects to a standard USB-port in the PC. It is supported of a software driver (USB-Agent) installed along with the SiPass Entro software is loaded when booting the computer.

There are also Kits available with the proximity reader PR500 (Cotag or EM4102 technology) together with a desk stand and USB-RIF/2.

3.5 Small applications – without LAN

SiPass Entro is designed for use in smaller applications with only a few doors.

Other than correct planning it is often necessary to take use of some dedicated cabling. You do not have to consider LAN, IP-addresses etc.

You just need some meters of cable, a SR35i, a Power supply and readers! It’s as simple as that!

3.6 Larger applications – with/without LAN

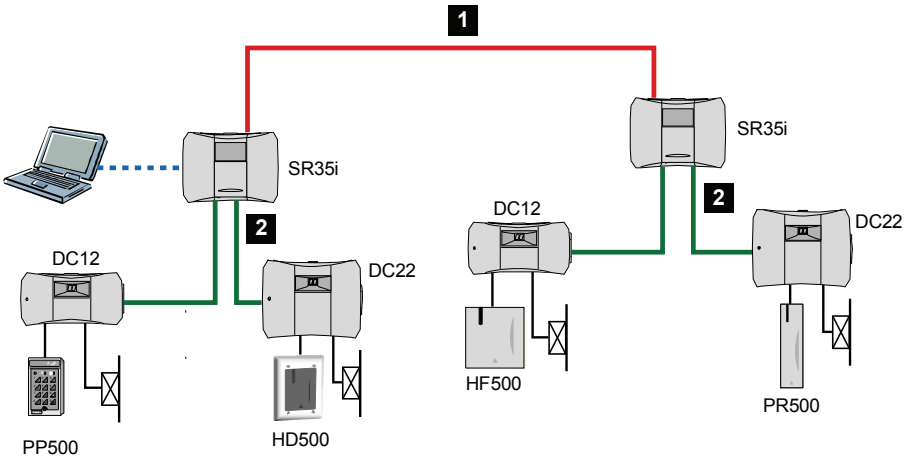
SiPass Entro has the capacity of handling up to 512 doors and 40 000 people in the same system (database).

In addition one PC can manage up to 10000 similar systems – via modem and/or LAN. These systems consist of separate, unique databases. They can however, be controlled and stored on the same PC.

The access control system should include one or several properties placed in different localities.

When one premises has many doors you can still use dedicated cabling. The system is split into separate sections managed by its own SR35i Segment Controller. This handles a couple of doors (local bus). All sub-systems are then linked into a higher level of communication (global bus).

Facility with RS485 cable



Facility with RS485 cable

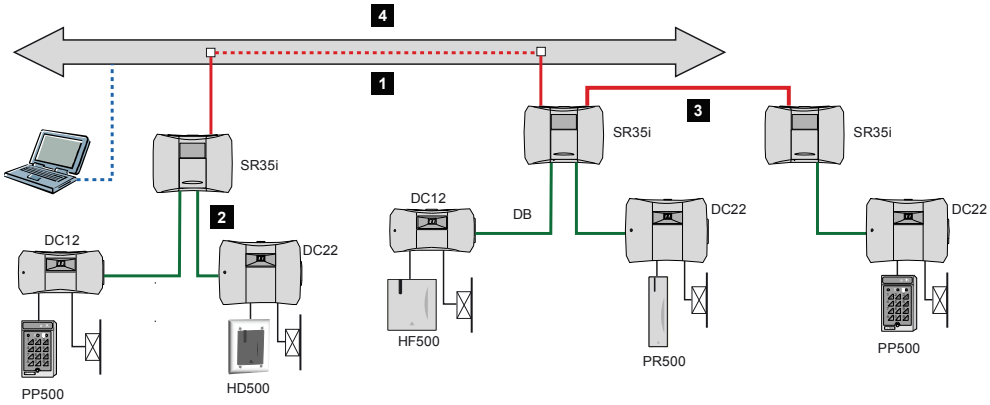
1.	Local RS485 bus
2.	Global RS485 bus

Both TCP/IP and RS485 use global communication

When several properties exist in the same system, a LAN may be considered. Note that the numbers of doors cannot exceed 512 in up to sixteen segment controllers.

In this case the global bus will be connected via LAN (TCP/IP) but each SR35i controls “its own” doors locally.

A combination of the two communication methods can also be possible as only one SR35i in the facility uses LAN whilst the others connect via traditional cable.

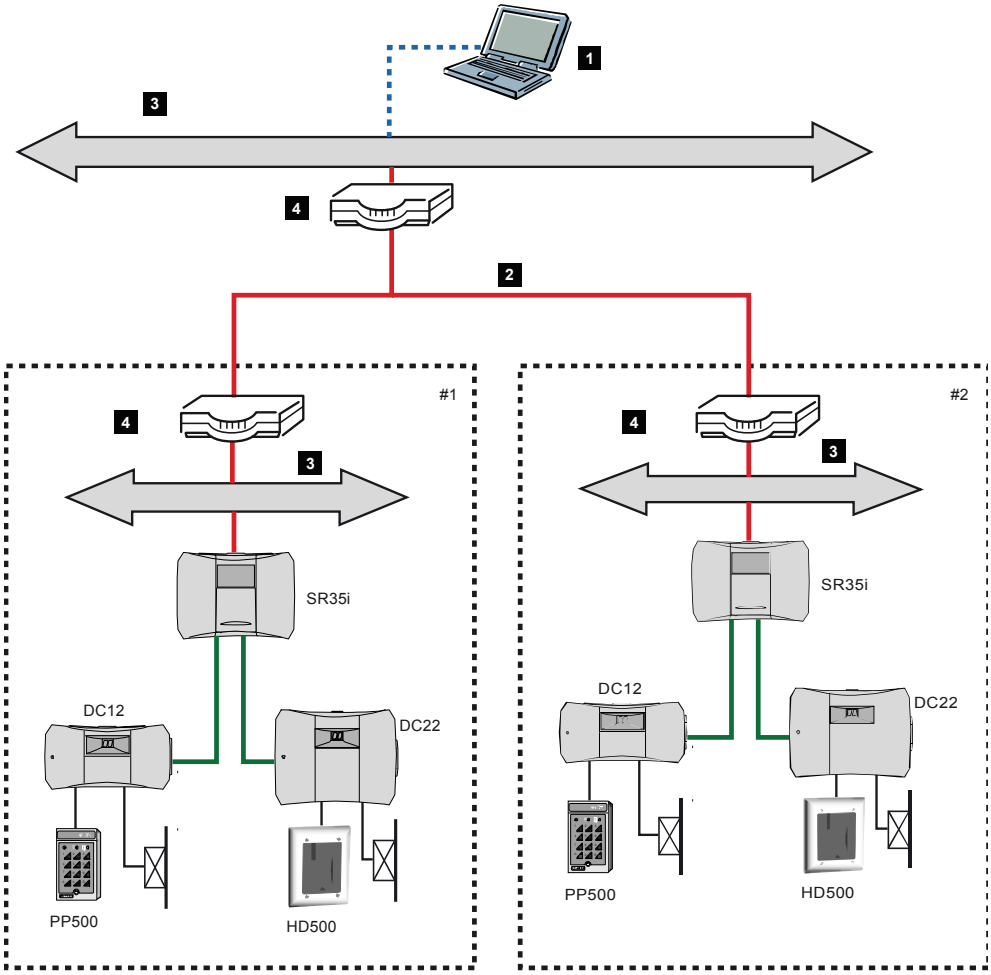


Both TCP/IP and RS485 in global communication.

1.	Global communication
2.	Local RS485 bus
3.	Global RS485 bus
4.	Local Area Network in same building (TCP/IP)

Two systems with separate databases

In some cases only a central PC can manage different, unique systems in different facilities. This can be obtained via modem or LAN. See figure – Network connected PC for two separate SiPass Entro.



Network connected PC for two separate systems

1.	PC with two different databases each with separate login
2.	Global network or Internet (encrypted TCP/IP)
3.	Local Area Network
4.	Gateway

3.7 Communication with PC

SiPass Entro SR35i offers three ways of communication with a **PC**.

By default the software installation assumes that only one computer shall log on to the system. If several computers (users) shall log on at the same time more so called connections must be setup.

3.7.1 Local Area Network

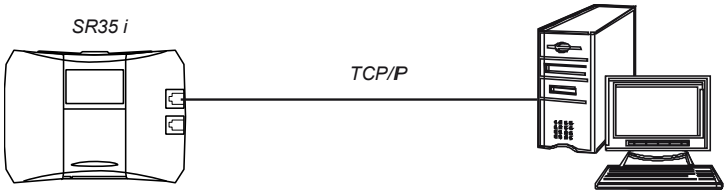
In this configuration, the Local Area Network (Ethernet 10/100 Mbit) is used for TCP/IP communication with the PC.

It is very important that the IT-manager of the end-user has participated in and has approved of all aspects of this part of the installation.

Note that the SR35i has an **integrated network switch with two connectors (RJ45)** where a PC and an SR35i can form a local area network without any extra equipment (except for the cable)

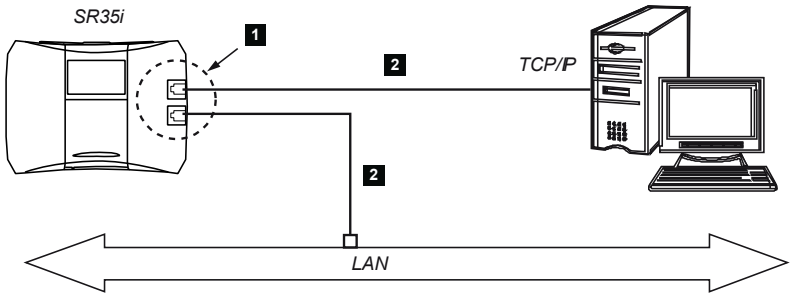
Directly connected – without LAN

In this case the PC has static IP address and is connected directly to the SR35i as an alternative to RS232 where longer distance (<100 m) is required.



Directly connected – with LAN

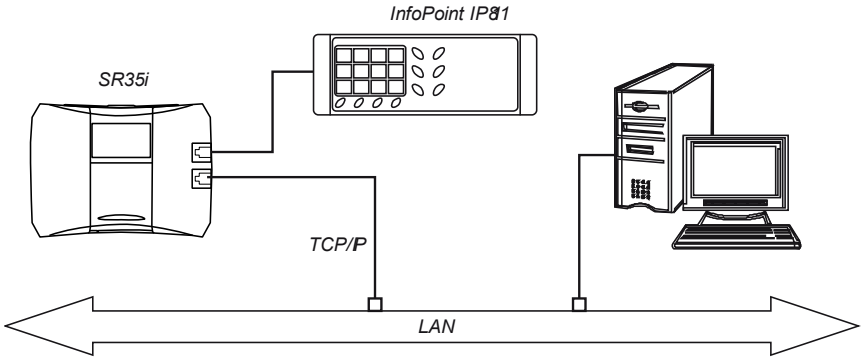
In this example the integrated network switch is also used to connect the PC onto the LAN.



1.	Integrated network switch.
2.	RJ45 type of cables.

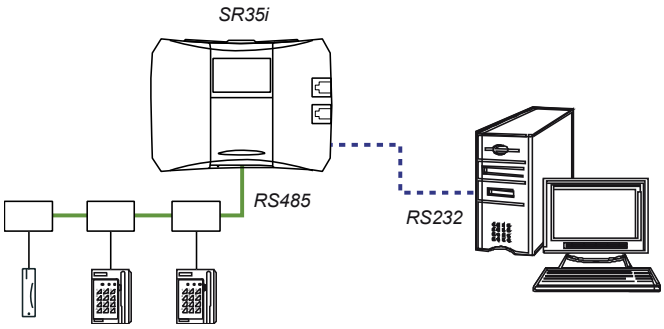
Local area network with InfoPoint IP811

The InfoPoint can be connected directly to the SR35i segment controller.



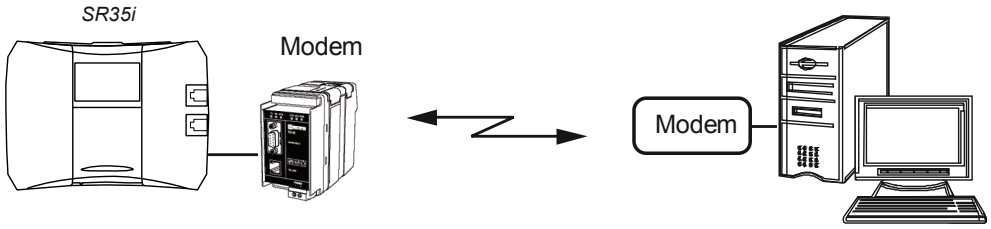
3.7.2 RS232

SR35i communicates with the PC via cable directly to the COM-port.



3.7.3 Modem

The PC is used to control a remote site using a dial-up modem. The SR35i is also connected to a modem, which also can dial up the PC if necessary.



3.8 Connect more than one PC

3.8.1 Multi-user database

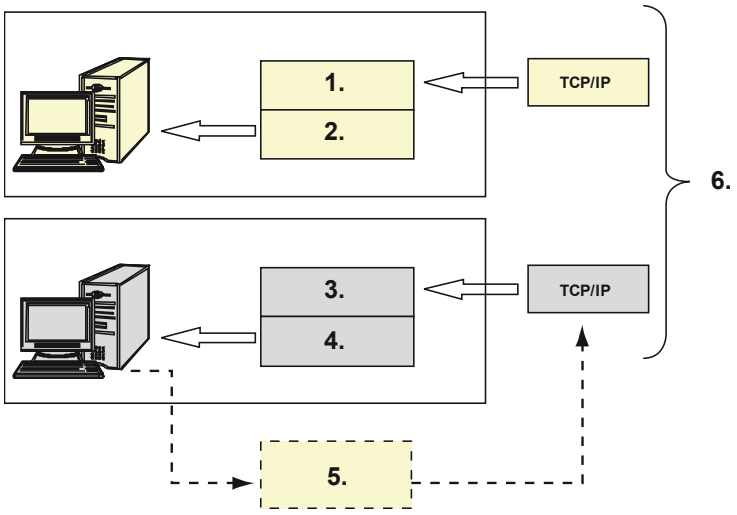
Every SiPass Entro system uses a **database** (with cards, time schedules etc.), which is stored in every segment controller and PC. The SiPass Entro database allows for **multiple users** to be working with the same database.

The prerequisites for this are that the system knows which Users are using which computer. E g a Security manager can have their own PC (with a dedicated license) while a Receptionist has another PC (with another license). For every PC there must be a 'connection' in SiPass Entro where the license number and communication ports are defined.

At the same time the applied filter events will only be sent to each PC respectively. I.e. if the Security manager temporarily log on to the Receptionist's PC no events will be received to this PC.

For every new System user you create you have to specify also the connection and which event filter is to be used.

The simplified illustration below shows how it works.



1.	Manager - Login
2.	Filter 1 - Events
3.	Receptionist - Login
4.	Filter 2 - Events
5.	*Optionally*: Manager – Login. **NO events received**!
6.	Connections to SiPass Entro system

Instead, if only one PC is used with several users the different filtered events will be stored in different folders on the PC (dependant of the user logged on).

3.8.2 Microsoft Terminal server 2008

The SiPass Entro software can be ordered as a Microsoft Terminal Server 2008 package which makes it possible to install SiPass Entro as a client-server application. Note that also MS Terminal Server 2003 is supported.

This means that the SiPass Entro software is installed on a central server PC. The Terminal server application will then allow for client PC to logon to the SiPass Entro programs.

More than one client can then be logged on concurrently and SiPass Entro manages all the database handling. A **license number is required for each client**. All events and information are stored centrally on the server and no data is stored locally.

Please refer to the special SiPass Entro *Terminal Server 2008 Installation Note* supplied with the SiPass Entro package for installation and configuring.

3.9 Global communication between several SR35i

The global communication between several **controllers** can be done through two separate physical cables – twisted pair **RS485** and/or **Ethernet 10/100 Mbit**.

3.9.1 RS485

Use RS485 to communicate between a maximum of 16 SR35i controllers. Maximum distance is 1200 meters from the first SR35i to the last one.

It is possible for one or more of these SR35i to use TCP/IP as described below. The controllers are then configured with an IP-address and proxy function (with SNTP).

3.9.2 Ethernet with TCP/IP

Generally known as TCP/IP that uses the Ethernet connection (10/100 Mbit) that connects to the Local Area Network. TCP involves a controlled way of sending messages through a network. The maximum distance depends on the structure of the network itself.

Requires that the SR35i is configured with its unique **IP-address** and having the **Proxy** function (with SNTP). This ensures that only the relevant units (SR35i or PC) receive the messages

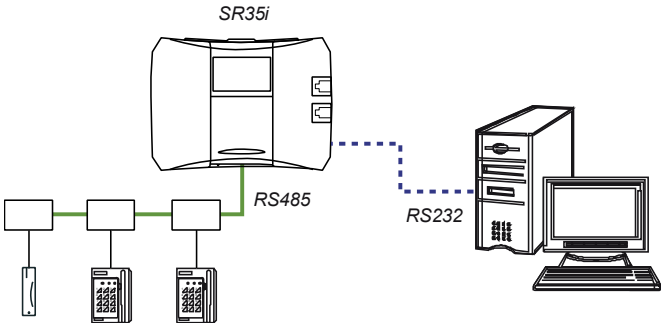
Notes when using SR35i and TCP

Remember that any zones (e g Alarm zones) will work best if they reside in the same sub-net when several SR35i use TCP/IP (between related SR35i).

3.9.3 Example of SR35i with RS485

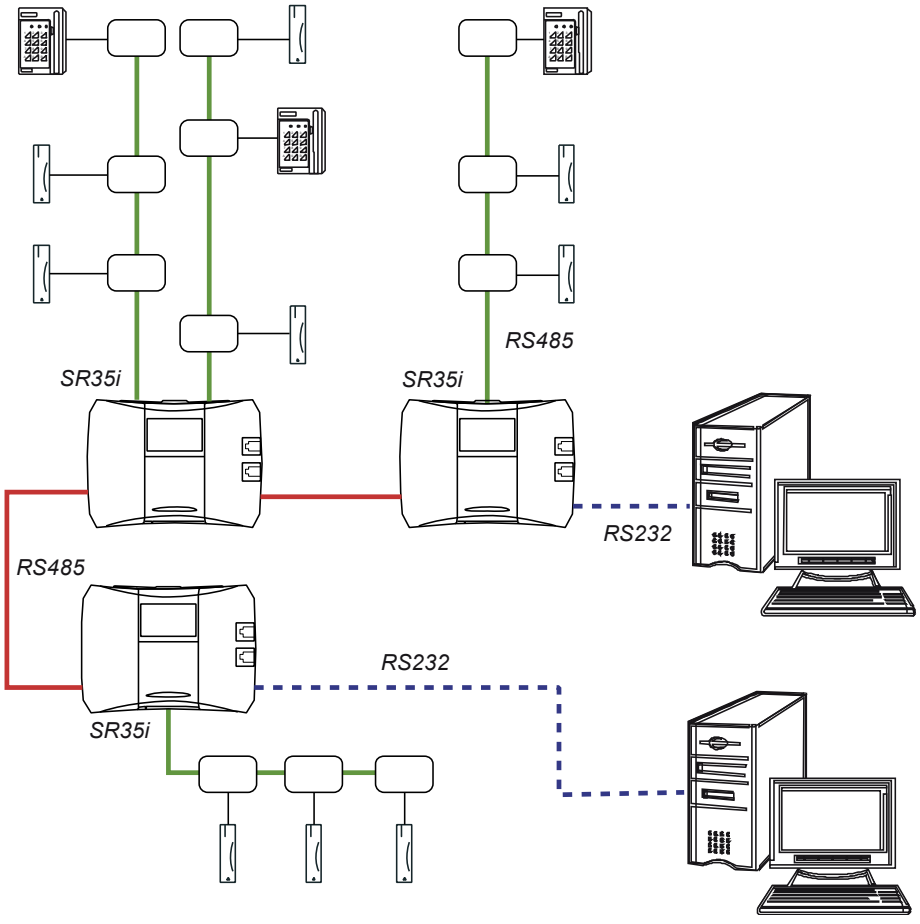
This solution gives a more closed system with dedicated wiring (RS485) between the segment controllers.

Small application – with one SR35i



Small system with only one SR35i

Larger application – with several SR35i

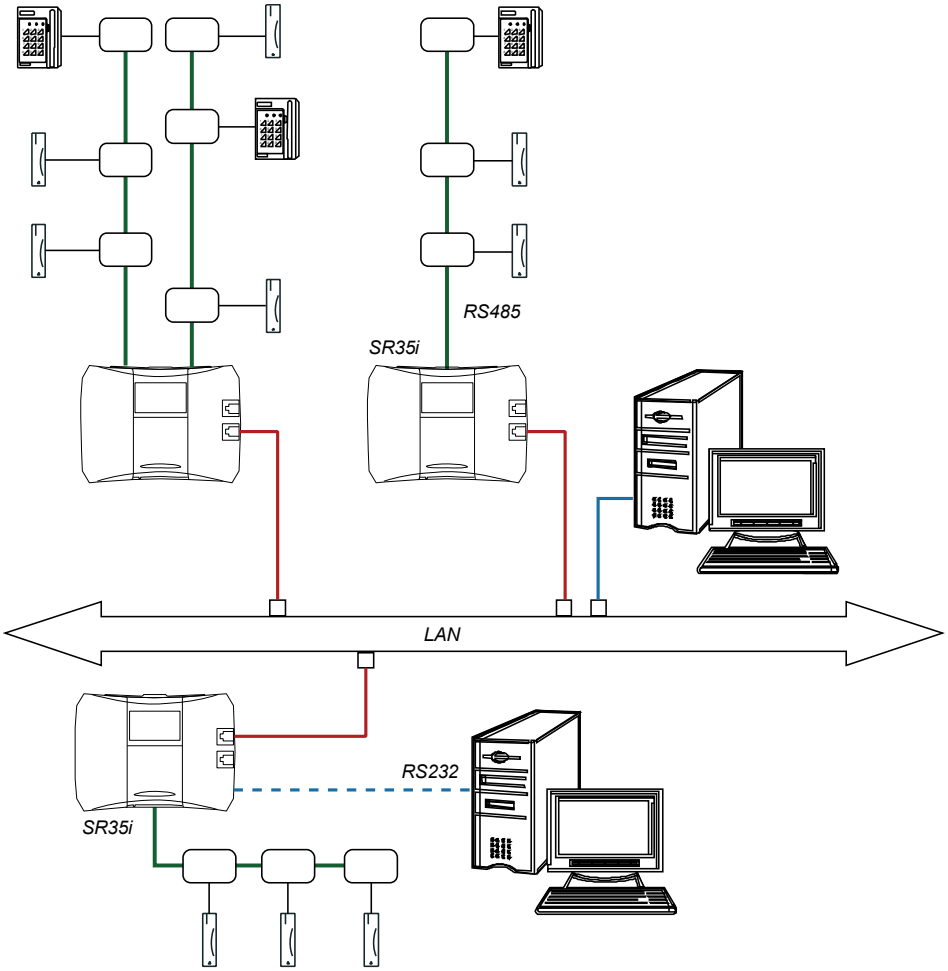


Several SR35i in a wired network

3.9.4 Example of SR35i used in Local Area Networks

This version of SiPass Entro gives the possibility that several SR35i can communicate through local area networks and the system can be software controlled from any PC on the network. No separate connections are needed between the controllers.

Note that it is possible to connect the PC directly (RS232) - or via the network.

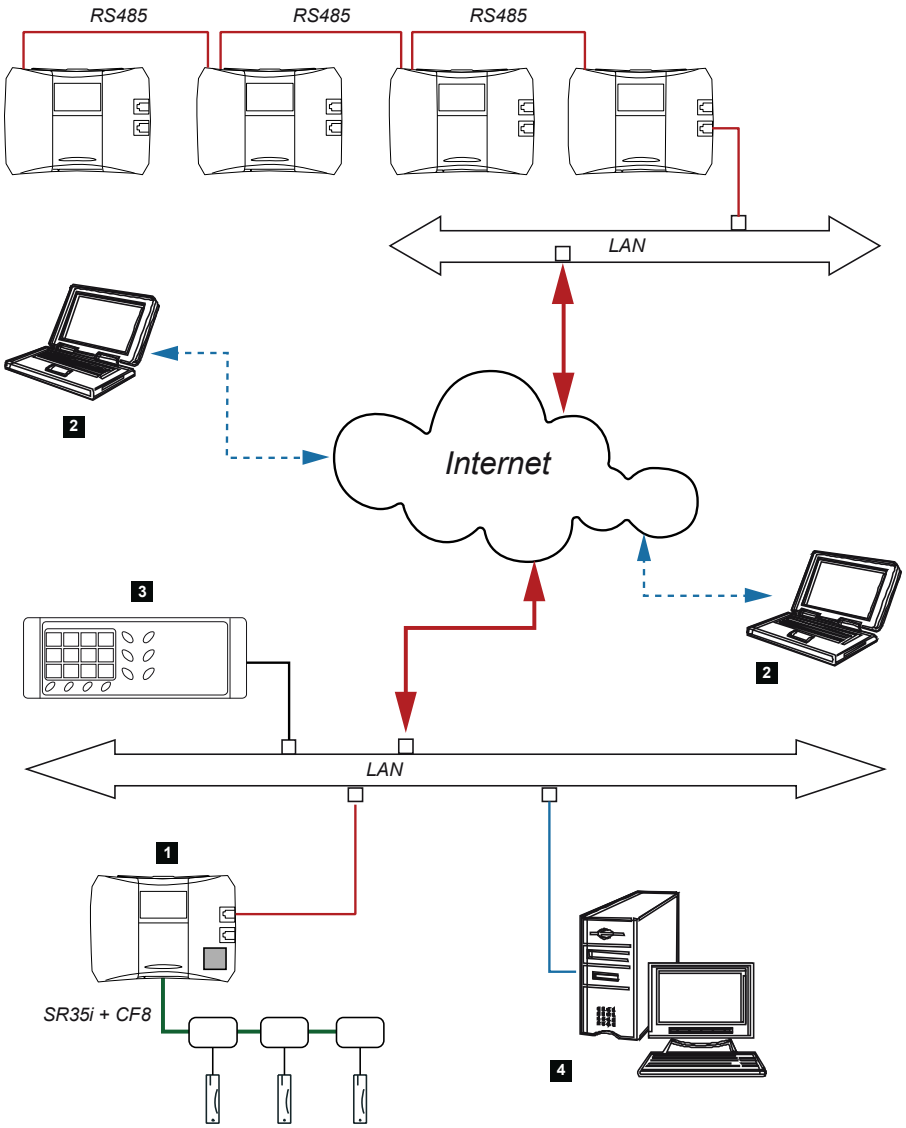


Several SR35i with TCP/IP communication

3.9.5 Example of SR35i using Internet

In this case the Internet, Local Area Network as well as RS485 are used for communication between units.

For example, some PCs can be used only for login to a Reservation system via the Internet – and other PCs could be used also for system administration



Internet based application

1.	Reservation Web server
2.	Reservation Web Browser (MS Internet Explorer)
3.	Reservation InfoPoint IP811
4.	Security Manager

3.10 Wireless communication

It is possible to use wireless communication (radio network) in the SiPass Entro. This can be applied between a RF-based battery-driven Codoor unit (RF30-EM) and the Segment controller SR35i.

Up to 512 wireless door environments can exist in the same system together with up to 512 wired doors. **One SR35i can manage both wired and wireless doors**.

Please refer to the product information for the RF30-EM to see the requirements.

E g Scandinavian style of lock cases.

The *Wireless Installation manual* describes further how to install the wireless application.

3.11 Reservation

SiPass Entro includes reservation functions (e g in sports arenas, tennis courts, conference rooms etc) and works together with the integrated access control system.

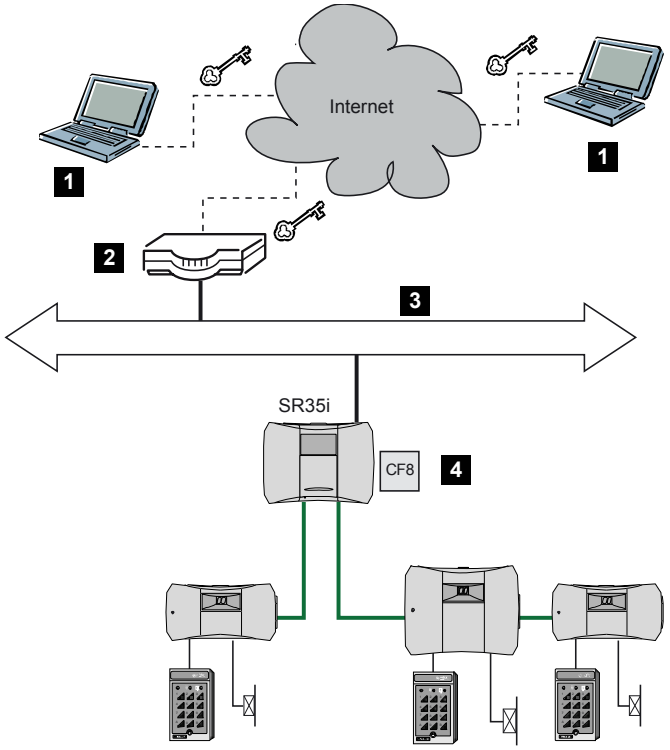
The System Administrator sets which objects (such as card readers/doors) are to be included and chooses the relevant reservation time schedules.

The users wanting to reserve times can use an ordinary web-browser (such as Internet Explorer) and login to the SR35i containing the reservation system. Alternatively use his/her card in a reservation terminal (InfoPoint IP811) – depending on how the system is configured.

3.11.1 Integrated Web server

The SR35i has an integrated (embedded) web server function, which is used for reservation applications. It requires that the dedicated SR35i have a permanent connection to the Internet (when Internet is used).

At least one of the SR35i must be equipped with a Memory card for web reservation which will contain the reservation information.



Example of standard solution for Reservation

1	Web browser
2	Gateway
3	Local Area Network
4	Memory card for web information (web server)

3.11.2 How the Reservation system is installed

First, all the doors and any IOR6 (for doors and machine control in the objects) are installed according to earlier sections. Afterwards the CF8 is mounted in the SR35i intended for reservations.

Depending on how the reservation function is specified, one or more InfoPoint IP811 or touch-screen terminals can be connected to the system through the network. I e a combination of PC and these terminals is possible. Technically the entire reservation information is stored in an integrated website (in a SR35i) with its own IP-address on a network. Configuring is described the User Manual.

The address to this website is **http//xxx.xxx.xxx.xxx/login.html** which should be notified to the users of the Reservation system.

3.12 Integrate CCTV system

The SiPass Entro software can communicate with up to 16 DVRs via TCP/IP. It supports DVR units in the Siemens SISTORE™ AX-, CX- and MX- range.

We recommend that the installer have good knowledge about DVR system in general and SISTORE™ systems in particular before any DVR functionality is introduced into the SiPass Entro system.

Implementation

The integration of DVR and SiPass Entro indeed consists of two separate hardware systems which are connected via TCP/IP and remote software functions. This means that you initially install software components for both systems in the same PC.

When you then configure functions (like filtered and timed triggering to start recording) in the SiPass Entro, these are then sent to the DVR. When the conditions for a certain action then are met the DVR starts recording images.

You may then replay these directly from the SiPass Entro Door monitor with some optional command options.

3.13 Integrating with external applications (BAPSI)

3.13.1 General

Normally access control system software is quite proprietary to its system components and is seldom open for customized applications. This is quite natural because it is also a security system to be used for controlling e g access to doors in different kind of facilities.

SiPass Entro can use a well-defined configuring interface to communicate with other, external software packages (like Time & Attendance, Alarm control or similar). E g to import/export cards, get time stamps or events.

An ordinary **TCP/IP** link is used for transferring the data between the different software components.

The external software must be modified/completed according to the specification we call BAPSI. Remember, this not a program just guidelines to the programming interface.

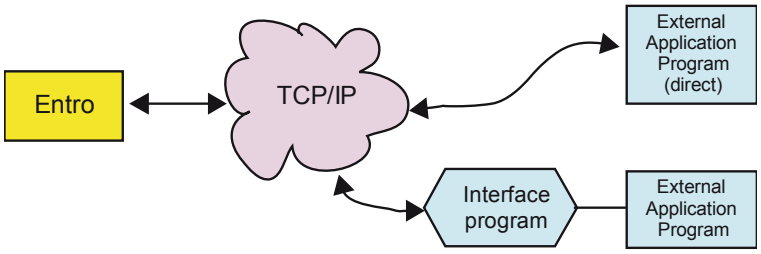
With BAPSI this is done in a specified and safe (encrypted) way that still keeps the access control system on a secure and integral level.

The specification can be requested from Siemens Building Technologies.

3.13.2 What is BAPSI used for?

Normally the User interface in access control software allows for functions like card registering, time schedule configuring and standard event logging (and searching).

Using BAPSI, custom application software can take advantage of sending/receiving messages to/from the access control system – and easily add new functions into the overall system. This could be Time& Attendance, Reservation systems etc.



3.13.3 Field applications

At the moment there are already systems running in the reservation applications area – using the BAPSI software interface. In this case the supplier of the external reservation software made a modification to their software module, which writes data into a file – and Siemens Building Technologies developed a special module that reads this file and forwards this information to the access control system

3.13.3.1 Application example - External Reservation system

Siemens Building Technologies have, mainly for the Swedish market, developed an application (based on BAPSI) called BAPSER, which allows for sending data between SiPass Entro and external reservation software (at the moment Idavall-Fri and Argentum-Booking).

The module is installed in the external PC that uses a TCP/IP link to send the reservations to SiPass Entro.

If you intend to use BAPSI in some way the SiPass Entro must have some parameters set up.

This is described in the documentation supplied with the BAPSER but you can invoke the menus by proceeding as follows:

1. Open the Installer application and click on **Connections**.
2. Click on **New**.
3. Select **BAPSI – external application integration** and proceed.
4. Enter the necessary parameters applying to the actual application.
5. Click **OK**

4 System requirements

Recommended minimum specification for PC:

- Processor 1 GHz
- 512 Mb RAM
- CD-ROM drive
- VGA colour monitor 1024 x 768
- Local Area Network connection (or serial port for connection of segment controller/modem).
- Windows 2000, XP, Vista, Windows 7 or Microsoft Terminal server 2008/2003 functionality. (We recommend that the latest available operating system Service Pack is installed).
- Citrix platform supported.

Basic requirements for network:

- Twisted pair Ethernet 10/100 Mbit connection.
- Communication between SR35i is done through TCP/IP.
- We recommend static/permanent IP-address for every SR35i (often also Netmask and Gateway are needed).
- We recommend permanent, active Internet connection of SR35i (when Internet is used).

Note - when Internet connection is used, the following ports have to be open (in fire-walls or similar) and configured as follows:

- 4002 if communication is used between PC and the chosen SR35i.
- HTTP (port 80) when using reservation via Internet.
- 4011 for TCP when several SR35i communicates through LAN.
- SNTP (port 123) for fetching correct time, if SR35i uses TCP protocol between each other.

4.1 Recommended system cables

The table below shows what kind of connections could be done in SiPass Entro.

Siemens Building Technologies will not warrant systems where other types of cable are used for these connections. Cable types must not be mixed in the different cable segments.

From unit	To unit	Type of cable	Maximum length (m)
PC	SR35i	**RS232** Cable between PC/printer and segment controller. Maximum length: 25 meters. Specified cable: Straight screened cable (4 + screen), e.g. Belden 9534.	25 m
	SR35i	**Network** Cat-5 cable, 10/100 Mbit. If in doubt - consult the IT-manager.	Depends on the network structure but normally 100 m to router/switch/hub.
SR35i	SR35i	**RS485:** The “global” circuit between the segment controllers. Specified cable: Pair twisted screened (1 pair + screen), e.g. Belden 9502.	1200 m
	SR35i	**Network**: Cat-5 cable, 10/100 Mbit. If in doubt - consult the IT-manager.	Depends on the network structure but normally 100 m to router/switch/hub.
SR35i	DC22 DC12 DC800 IOR6 PD30-EM PD40-EM	**RS485**: The “local” circuit between a segment controller and its subordinate door readers/door controllers. Pair twisted screened (1 pair + screen), e.g. Belden 9502 or Cat-5 (communication) and 1.5mm^2 (power) **OR** PAARFLEX CY (custom cable comprising communication and power in one cable).	1200 m
DC22 DC12 DC800	BC43 M43 PR500 HD500 SP500	**BC-Link:** Specified cable: Straight screened cable (4 + screen), e.g. Belden 9534	100 m

From unit	To unit	Type of cable	Maximum length (m)
	PM500 PP500		
	HF500 BC5511	**Clock&Data:** Specified cable: Straight screened cable (6 + screen), e.g. Belden 9536.	50 m
	Wiegand readers	**Wiegand:** Specified cable: Straight screened cable (6 + screen), e.g. Belden 9536	50 m

4.2 Cables

SiPass Entro can be operated using different cable types for the communication levels, as well as for the power supply.

4.2.1 Cable for power supply

In both large and small systems it is important to use the dimensioned cable correctly. The most important factor to consider is that the cable is linked to the door environment. In most cases it will be the electrical locks that will consume the most current and could cause a drop in voltage. This is why it is necessary to know the types of locks; (lock strikes, motor locks etc.) when dimensioning the cables.

In most access control systems there are some kind of centralized power supplies such as battery-backup. When using these methods it is very important that there is a large enough area of cable. We recommend an area of at least 1.0 mm².

This will exclude data cables such as ELAKY, Belden, CAT-5, CAT-6, CAT-7 etc. as they have areas around 0.1 – 0.2 mm²) and will not fit the purpose of a power supply. A popular cable is the ”combi-cable”, which is a PAARFLEX with 2 x 1.5 mm² (also with a pair 2 x 0.5 mm² aimed for data communication).

See more about Power supplies [→ 38] for advice on how to plan the cable network.

4.2.2 Cable for RS485

Between SR35is, and door environments, cable should be specified for RS485. It is important that the cable is screened and twisted. In both cases the maximum length is 1 200 m.

If each SR35i is powered by its own power supply, only a simple data communication cable between them is sufficient. E g the “combi-cable”, ELAKY, Belden - or similar.

However - if two SR35is are to be powered from the same supply another pair of cables are needed. The “combi-cable” is sufficient. It is also available with two pairs of communication wires.

4.2.3 Cable for network (TCP/IP)

If LAN is used as a communication between a PC and a SR35i – or between SR35i – some existing LAN cable will suffice. Cat-5 cable (specified for 10/100 Mbit) is mandatory.

Note that the SR35i have an integrated network switch with two external connections and one internal for SR35i. This means that you can use a standard network cable – without any hub – direct to PC and/or local area network.

Whether new or old cables are used the customers IT-manager must be consulted when specifying or commissioning up the system.

4.2.4 Cable to PC

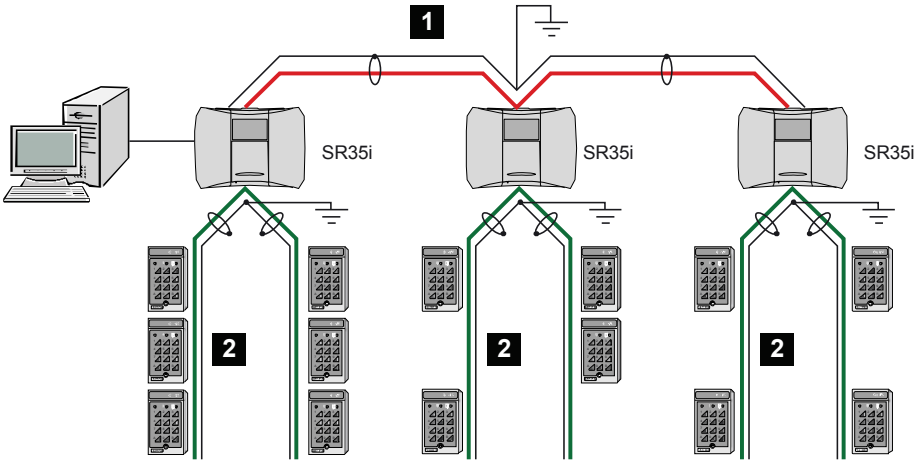
Between the SR35i and the COM-port on the PC a straight RS232 cable is used.

For LAN use a common, standard LAN cable (Cat-5 Ethernet).

4.2.5 Earthing and screening for RS485

The cable screens on each circuit must be connected to protective earth, **but only in one place** in the system (see diagram). Also remember that metal parts in doors or vehicle barriers can be in contact with earth. For readers installed on these surfaces, the screen must not be connected to the metalwork.

Avoid placing the cables close to heavy current installations, (e.g. lifts and power doors) since they may cause disturbance.



Connection of screen

1	Global bus
2	Local bus

5 Power supplies

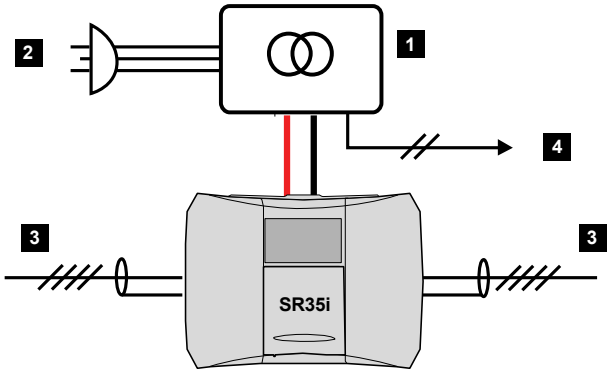
5.1 Central DC power supply

Central power supplies are often used to power an access control system. Here are some advantages:

- Stable 24 (or 12) Volt to electrical lock (which normally only accept +/- 15 %).
- Backup power for locks when main voltage falls.
- An alarm can be generated if main voltage falls and battery powering starts.
- Fewer units to install.
- Easier to expand the system (if enough margin from the start).

Note that SR35i has a lithium battery that keeps data when power disappears.

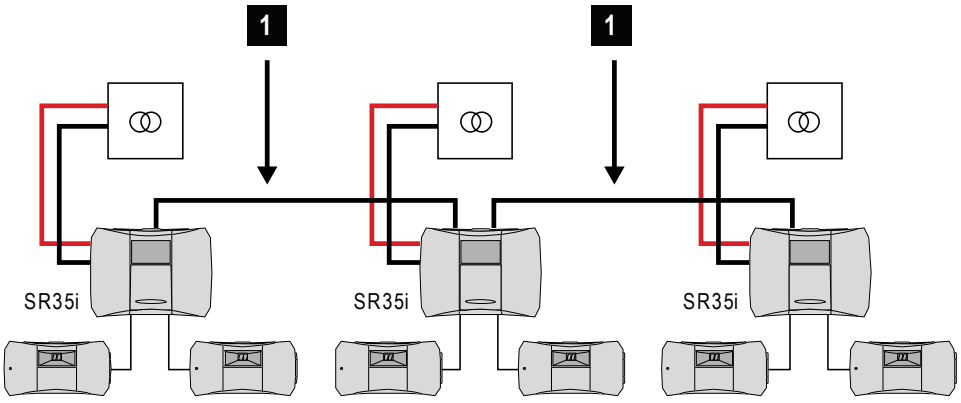
Connect the power supply according to the instructions below, but do not connect the power to outgoing cables.



1.	Power supply.
2.	Mains 2 + earth.
3.	Local bus (4 + screen).
4.	Power supply failure connected to IOR6.

Isolated communication

The main idea is to form a system such as that illustrated in figure below, where every segment is powered separately. If this is achieved the risk of earth current is minimized because the only existing link between the segment controller is a galvanic, isolated RS485. Note that also TCP/IP LAN means isolation between SR35i.



Isolated communication when using central power supplies

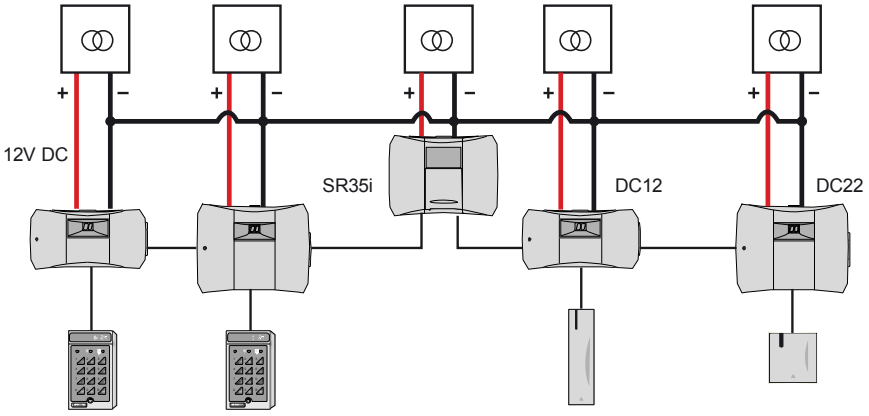
1	Global, isolated RS485 communication

5.2 Local DC Power Supply

Whenever using separate power supplies for SiPass Entro for one or several readers, it is very important to **wire all minus (0V)** cables together. This is because the RS485 communication interface uses the minus potential as a reference. If there is voltage differences between the units there might be unwanted disturbance of the communication.

Be sure that the PSUs have a stable voltage output. Even if the SiPass Entro-system components are tolerant to voltage fluctuations, the locks may be more sensitive.

Also remember to use enough area of the power cables – especially if there are long distances involved. Below is an example of a 12V application where the SR35i is powered with a local power supply.



Local Power Supply

5.3 Voltage drop

SiPass Entro tolerates voltage levels down to approx. 10V DC for working whilst a 24V electrical lock might have a tolerance of maximum +-15 % which means that the voltage cannot drop below 20.4 V DC.

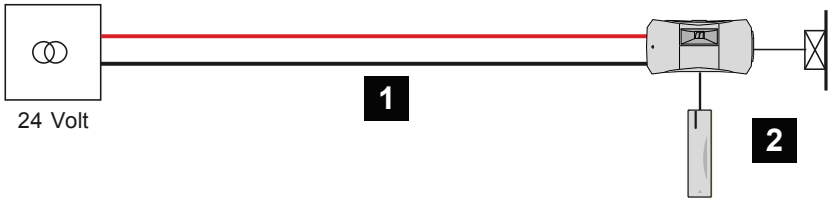
The calculation of voltage drop in cables is achieved by using Ohms law, which states:

Resistance (Ohm) x Current (A) = Voltage (V)

The parameters affecting the voltage drop are as follows:

- Current consumption at each unit (Ampere)
- Cable area (mm²)
- Length (m)
- Resistance factor for chosen cable (ohm/m)

It may be easier to understand voltage drop by using a simple example



Example of cable

1	100 m System cable
2	DC12+PR500 with lock strike

Method of calculation

Note! Always calculate with nominal battery voltage 24V (or 12V) despite a battery backup, output voltage may be higher – and maximal load at the units.

Current consumption at reader + lock (Ampere) = 0.160 A + 0.100 A = 0.260 A

Cable area (mm²) = 1.5 mm²

Length (m) = 100 m x 2 (both directions) = 200 m.

Resistance factor for system cable (ohm/m) = 0.0112 ohm/m

Resistance: 0.0112 ohm/m x 200 m = 2.24 ohm

Current: 0.160 A + 0.100 A = 0.260 A

Result: 2.24 ohm x 0.260 A = 0.58 V voltage drop. I e. 24.0 V – 0.58 V = 23.42V at lock. This is sufficient for a 24 Volt electrical lock.

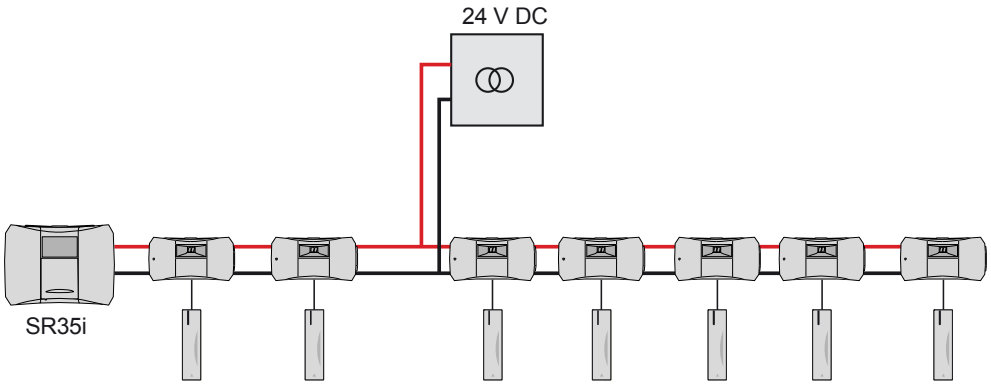
Result with 12V DC system

In many cases a 12V application consumes more current than in the case of 24V. With this in mind we assume that these units need 0.5 A.

Result: 2.24 ohm x 0.5 A = 1.12 V voltage drop. I e. 12.0 V – 1.12 V = 10.88V at the lock which is on the margin but still is sufficient.

5.4 Example of a typical power supply section

By placing the power supply, (such as a 24V) in the middle, you gain a better balance in the load and a better margin can be achieved.

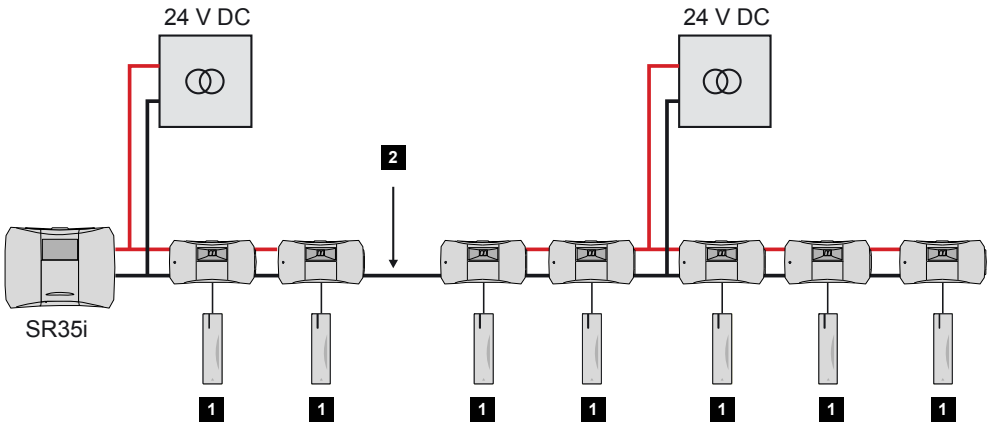


Typical power supply section (24V)

5.5 Several DC power supplies in the same cable section

Sometimes one power supply is not enough for securing power to all units in the same system section that a SR35i controls. If several power supplies are to be installed the minus (negative) wire must be tied between them. (This is similar to using local power supplies described in earlier chapters).

If this is ignored, the data communication (RS485) to/from door environments may be risked because the minus is used as a reference.



Several power supplies in same cable section

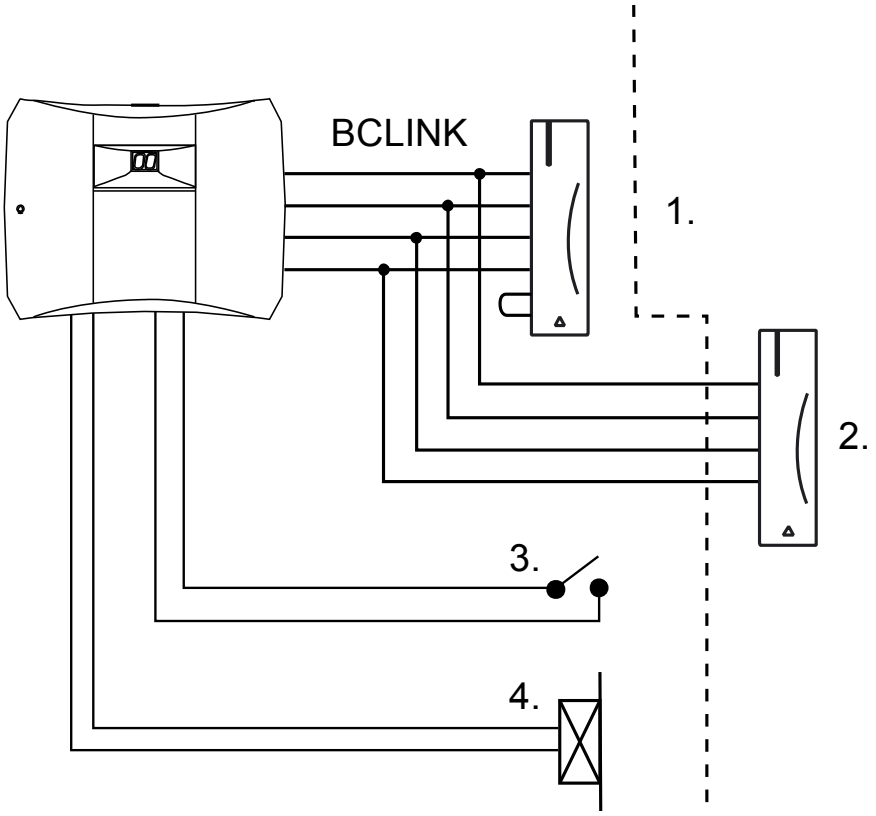
1	DC12+PR500 with lock strike
2	Must remain - used as a reference for data communication

6 Special installations

6.1 Anti-pass back using BCLINK readers

When BCLINK readers are installed for anti-pass back function a sub-addressing technique is used. This means that e g in a PR500, for example; The ENTRY PR500 and the link for EXIT PR500 are controlled internally by the door controller that decides upon the direction.

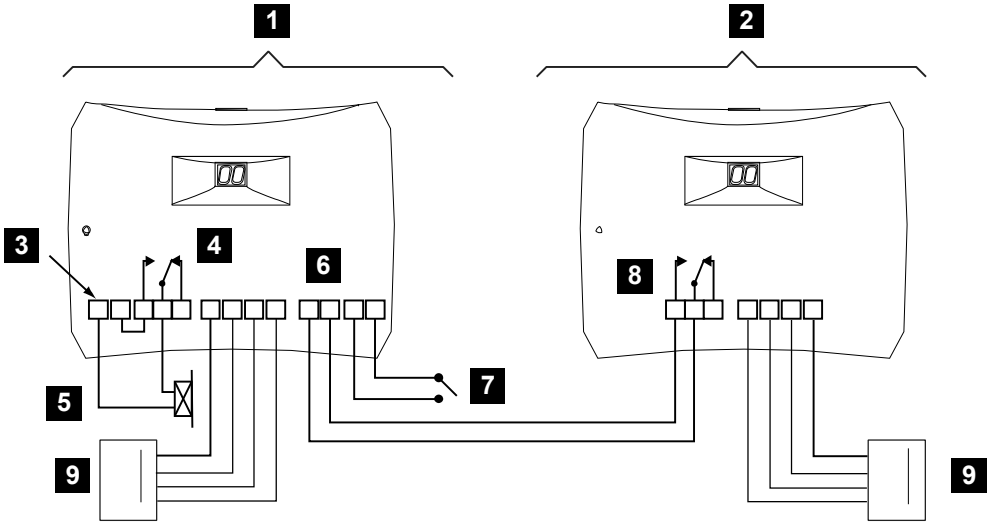
Wiring the door monitor contact and lock are done as usual.



1.	EXIT reader
2.	ENTRY reader
3.	Door monitor contact
4.	Electric lock

6.2 Anti-pass back using Clock&Data and Wiegand readers

If the readers do not support sub-addressing the door monitor contacts and opening relays are connected as follows:



1.	ENTRY (into the zone)
2.	EXIT (out of the zone)
3.	Power supply
4.	Opening relay
5.	Lock
6.	Remote opening
7.	Door contact.
8.	Opening relay. Note! Voltage free contacts
9.	Reader

Only connect the door contact on the ENTRY reader. Connect the EXIT reader's opening relay with voltage free contacts to the ENTRY reader's remote opening input. If needed, enable event registration of "Valid access – Exit button" in SiPass Entro event filter settings.

Note that only the ENTRY door controller monitors that the door is physically opened. The EXIT door controller registers the granted access (from the zone) but cannot monitor the door opening. If this is required we recommend that another solution with **one controller** with two BCLink readers [→ 42] (sub-addressing) are considered.

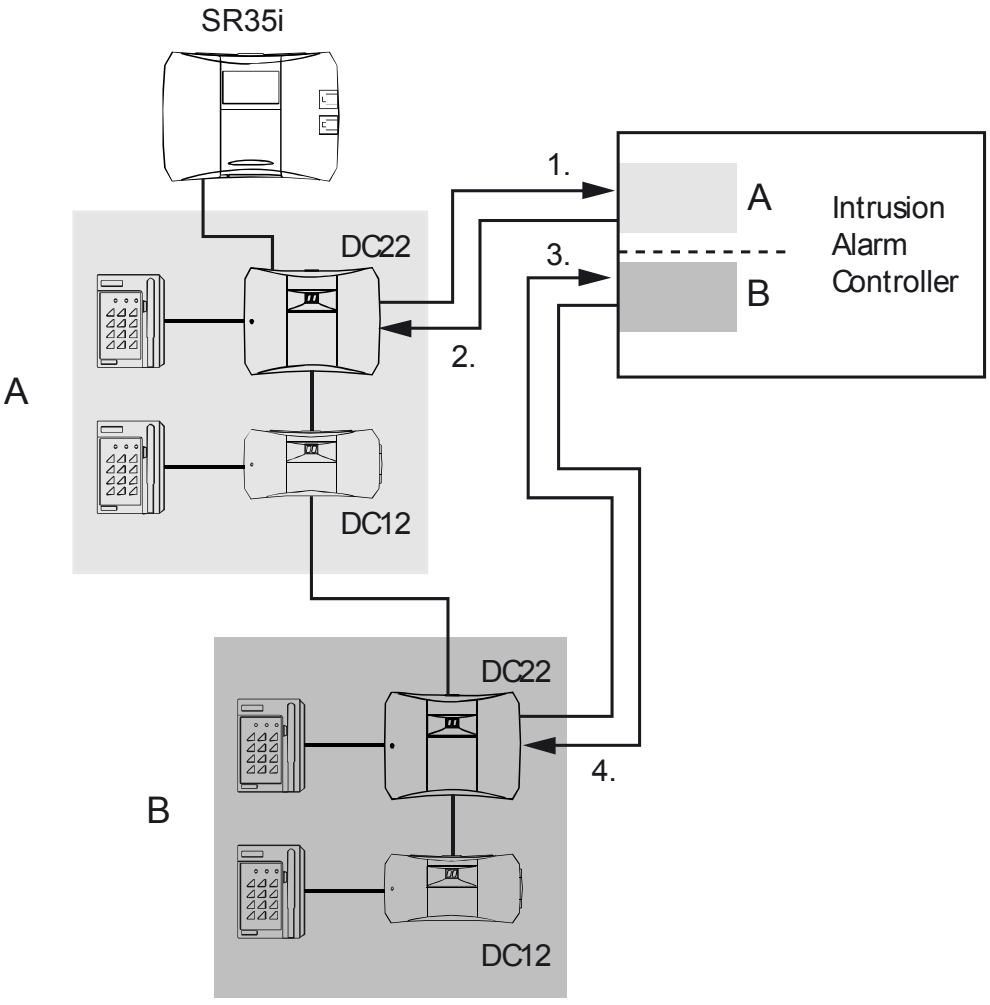
6.3 Intrusion Alarm Zones with DC22

The DC22 door controller must be used if any bistable intrusion alarm system shall be controlled by the SiPass Entro system.

To gain highest security, you normally install and use **card readers with PIN-pad** in all doors that are used for entrance to the particular section of the intrusion alarm system. You may then use the security level Card for arming the alarm and Card+PIN for disarming.

If any section area of the intrusion alarm system includes several doors, the SiPass Entro must be configured with one or more **Alarm zones**. Each zone must then consist of at least one DC22 (with the relay) while the other doors can remotely control it via the SiPass Entro system bus.

The illustration below shows how two separate zones may look like:



Example of Alarm zones

1.	Arming signal for Zone A (from DC22)
2.	Status signal for synchronization between systems (to DC22).
3.	Arming signal for Zone B (from DC22)
4.	Status signal for synchronization between systems (to DC22)

6.4 Connecting Alarm Status Feedback in DC22 (ASF)

When the DC22 is used to synchronize SiPass Entro and an external intrusion controller a feedback signal *from* the intrusion system can be used. Depending on the status of the signal, the SiPass Entro recognize the intrusion system as activated or deactivated and perform relevant operations as e g “blocking” or locking doors.

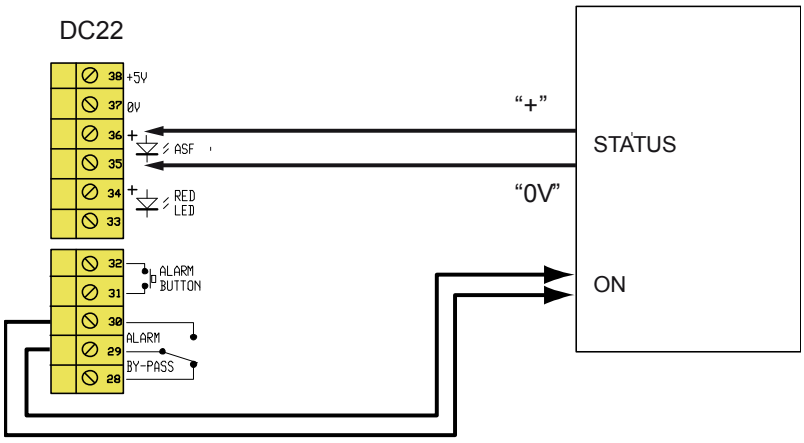
The connection between the systems can be done in two ways:

- With a voltage signal.
- With closing signal (voltage free).

Below drawings shows the different methods which both controls the input (ASF).

With voltage signal

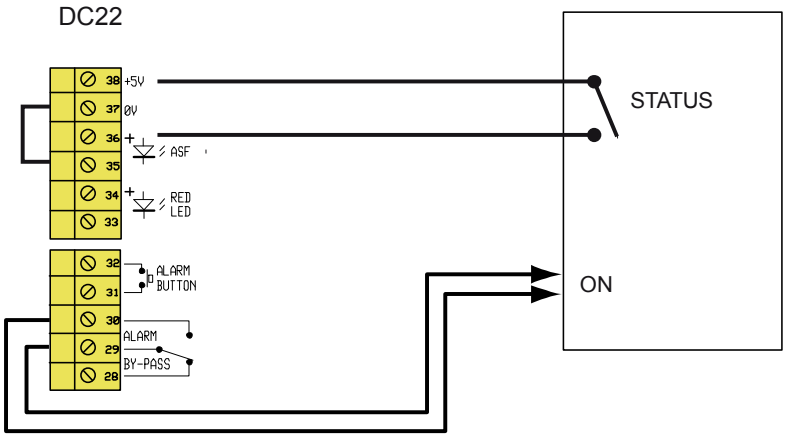
In this case the intrusion controller must send a voltage signal (maximum 24VDC) and a minus reference must be available.



Voltage controlled ASF.

With closing signal

The intrusion controller makes the closing. Note that a jumper has to be installed in the DC22 between 35 & 37.



Closing signal ASF.

7 Quick start guide

Although SiPass Entro includes many different functions to fulfil different customer requirements, the steps to form a basic Access Control System are not so many.

Below is a list of issues to perform to quickly get the SiPass Entro system work:

- Install software in the PC [→ 55]
- Set time & date [→ 79]
- Configure names for segment controllers [→ 83] & Configure SR35i [→ 86]
- Decide on time functions
- Configures names and functions for doors [→ 91] & Configure doors*
- Configure Access groups*
- Logging on card holders*
- Card printing*
- Configure System users*
- Access registration*
- Viewing status & events*

If you intend to use other functions – please read appropriate sections for further information.

- Intrusion alarm control [→ 97]
- DVR integration & Camera control*
- Reservation functions*

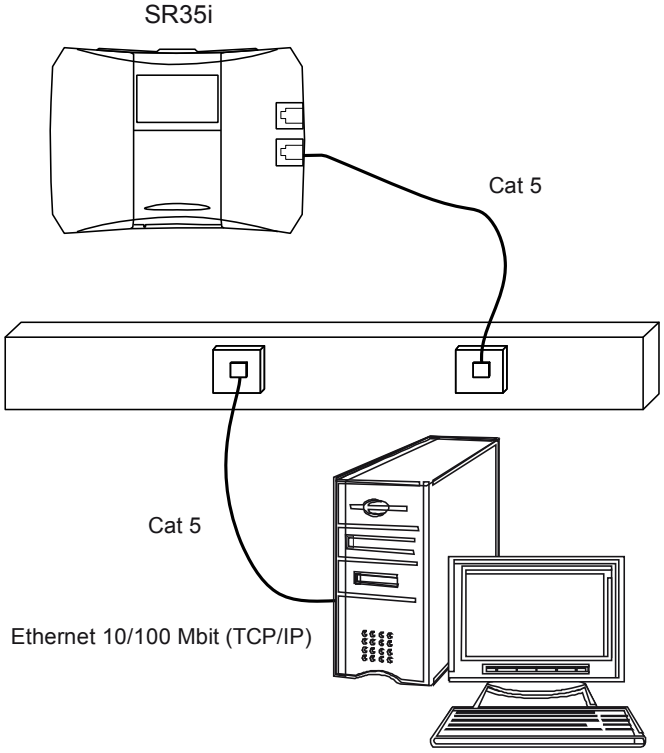
* To be found in other documents

8 Connect the PCs or an online printer

8.1 Connect PC via Local Area Network

By using the Local Area Network you must confirm with the IT Manager the correct IP-addresses and installation settings for the system.

1. Connect the Ethernet cable to the PC and the Local Area Network.
2. Connect the Ethernet cable to the SR35i and the Local Area Network.



Example of connecting a PC via Local Area Network.

Install a dummy network

It is also possible to form a dummy “local area network” which only consists of a directly connected SR35i and a PC. In this case you use a network cable between the PC and the network switch in the SR35i.

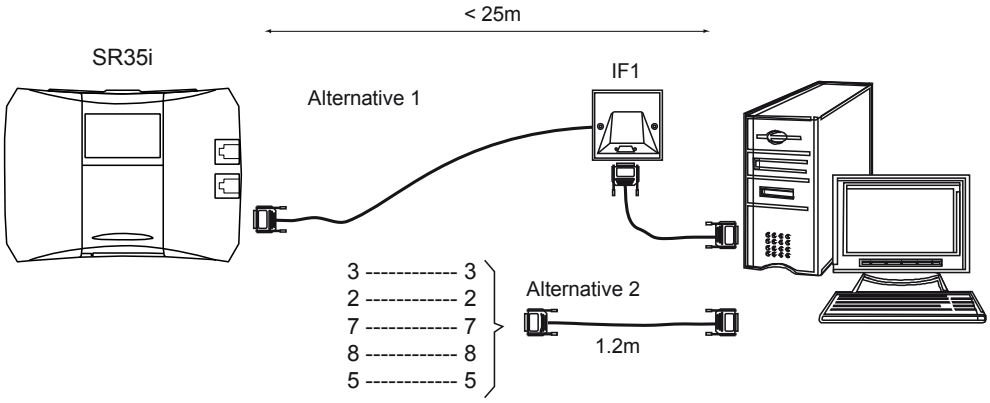
If you connect a temporary PC with network cable direct to SR35i, we recommend that also the PC use a static IP-address. Preferably in the range 10.1.200.xxx (with Netmask 255.0.0.0) because the SR35i initially is set to an IP-address in this range.

8.2 Connect PC with direct cable (RS232)

The segment controller must be installed close (max 25 meters) to the PC.

The illustration below shows an available, complete kit consisting of a wall socket (IF1), a standard RS232 cable (approx. 1.2 m) and 25 meter cable with one free end to connect to the screw terminal block of the wall socket. You can use the standard cable directly (alt. 2) between the PC and the SR35i - or make a more fixed installation (alt 1.).

RS232 needs fewer settings in the PC, which simplifies the set-up. You can also temporally use RS232 – and then change to Ethernet later.



Two alternatives for RS232 cabling.

The total distance between PC or printer and the segment controller must not exceed 25 meters maximum.

The RS232 port can also be connected to a printer. Note that either a PC **or** a printer can be connected to a segment controller – **not** both.

8.3 Connect an on-line printer (RS232)

To set up an on-line printer to print events directly from a SR35i, please proceed as follows.

1. Open the Installer [→ 76] application.
2. Go to **System settings > Connections** and enable multiple connections.
3. Select **New**.
4. Select **Printer for event logging** and click **Next**.
5. Define **name** for the connection.
6. Specify which SR35i that the printer is connected to.
7. Specify event filter to use.

The following parameters apply for the RS232 interface.

– 9600 baud alt 57 600 baud.

– No parity, 8 bits, 1 start bit, 1 stop bit, Printer output with hardware handshaking (character table ISO 8859-1).

9 Prepare any network resources

Before you install the software there are some resources that need to be defined and configured.

Also remember that some SR35i requires that DHCP must be configured via the SR35i menu system [→ 90] .

The End Users/Buyers IT-manager should always participate in the planning of a TCP/IP based SiPass Entro system. General knowledge about networking is also recommended.

9.1 Background

Static IP-addresses

Static IP-addresses can exist in both local area networks and/or where also the Internet is used (e g for reservation functions). Some ISP unfortunately do not allow for using static IP-addresses.

In a local area network environment the only aspect is how “isolated” the security system should be compared to an office network. I e if any routers, firewalls or similar software are separating the SiPass Entro from any other network equipment.

Dynamic IP-addresses

In earlier versions of the SiPass Entro software, the segment controllers was supposed to be addressed with a static IP-address – which is still the preferred method as long as the local area network (LAN) allows for this. (Think of a having the same telephone number all the time). Static IP-addresses are both faster and more secure.

In some facilities only one Internet Service Provider (ISP) is contracted, offering only accounts and connections using **DHCP** (Dynamic Host Configuration Protocol). This means that the host environment (at the ISP) “lease out” an IP-address for a short time, therefore the IP-address can be changed when the ISP renews the lease time.

As IP-addresses are not static, there must be a function that refers to a fixed name which can be “translated” to a concept the Internet can still understand – i e IP-addresses. This function is generally called **DNS** (Domain Name Service) and can be seen as a “name directory” with IP-addresses. The directory normally resides with the ISP and will itself also be accessed through an IP-address (which normally is supported together with the leased IP-addresses).

When DHCP is used – and the ISP often changes the connected users’/computers’ leased IP-address – also the DNS must be updated with new information. This is called **dynamic DNS** (DDNS) – and means that equipment can “ask” this service for the latest IP-address for a specific name.

9.2 Subnet agent (SR35i)

The “**subnet agent**” is a term used for a **dedicated SR35i** which administrate the communication between SR35i controllers who reside on a subnet of a local area network (where routers are used).

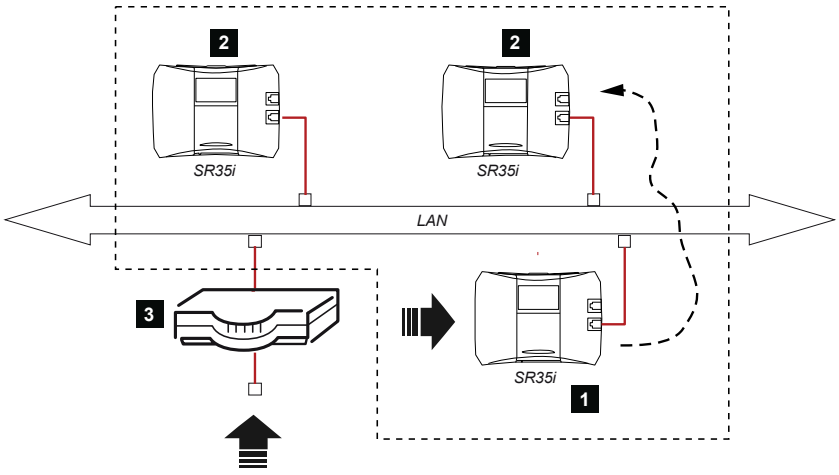
Only the IP-address of the router is visible outside the router. The subnet agent solves this by administrating the traffic to the other SR35i on the subnet.

The router [→ 51] is configured with the relevant parameters of the subnet agent.

If the subnet agent is using DHCP the MAC address must also be known, so that the router gets the “physical” identity (= MAC) of the SR35i.

Proceed as follows:

1. Power up the actual SR35i.
2. Press buttons **2** > **2** > **1**.
   ⇨ The **MAC address** is displayed as 12 characters. Note this down for further use.
3. Press ESC.
4. Press buttons **2** > **1** > **1**.
   ⇨ The **IP settings** are displayed. Note this down for further use.



Example of a subnet with a router

1.	One SR35i is acting as subnet agent for the subnet (dashed).
2.	The other SR35i are managed by the subnet agent.
3.	Router where ports are opened and the IP address and/or MAC address is configured for routing.

9.3 Router setup

Any router used in a SiPass Entro system need to be setup to manage the communication correctly. This means that the ports used in SiPass Entro must be opened. See the handbook for the router in use how to change settings.

Proceed like this:

1. Confirm the **IP address** for the dedicated subnet agent (SR35i). If the subnet agent uses DHCP, also the MAC address [→ 50] of the same SR35i must be known.
2. Configure the IP address and/or MAC address into the router so that the router knows where to route the information sent on ports related to SiPass Entro.
3. Configure the **ports** according to below:
   TCP-4002: Communication from PCs.
   TCP-4011: Communication between SR35i
   TCP-80: Reservation functions (If used).
   UDP-123: Network time functions.
4. Repeat the above if any other router used in the system.

DynDNS reporting in router

If the router has the option to also manage the reporting of a dynamic DNS [→ 51] , it could be used as a good alternative. Instead of using each SR35i for this.

If the router is used for reporting, a subagent (SR35i) must have the very same identity as the router.

9.4 DynDNS

Whenever the SiPass Entro will be using a DHCP server/router for IP settings a function for “dynamic” DNS (Dynamic Domain Name Service) must be established. The DynDNS functionality must be used to keep the identities intact for the SR35i controllers.

There are two options to report to a DynDNS service:

- Use the router (if possible) to report. Note that the identity chosen for the router must be the same entered in the SR35i (subagent) identity. See the router’s handbook how to configure the DynDNS function in the router.
- Use a SR35i to report.

In both cases the DynDNS service must be established.

9.4.1 Configuring of DynDNS.org

Currently the instructions to configure an account with dyndns.org. are as below. You can read more about this on their web site by browsing to, www.dyndns.org. (www.dynDNS.com)

1. Create a new account (User name and Password).
2. If you have your own domain you select Custom DNS – otherwise select **Dynamic DNS**. These choices will later be referred to in SiPass Entro.
3. Choose among the available domain names. If you chose **dynalias.net** a SR35i will get the network identity Identity1.dynalias.net.
   It will be easier if you already have a list of network identities for all SR35i available. Note that this is not the same as the name of the controllers (as shown in an event log).
4. Carry on entering the identities for the remaining SR35i that will use DynDNS. Remember that when a subagent (SR35i) is used for managing other SR35i behind a router, only the subagent needs to have an identity. But then exactly the same identity as the router.

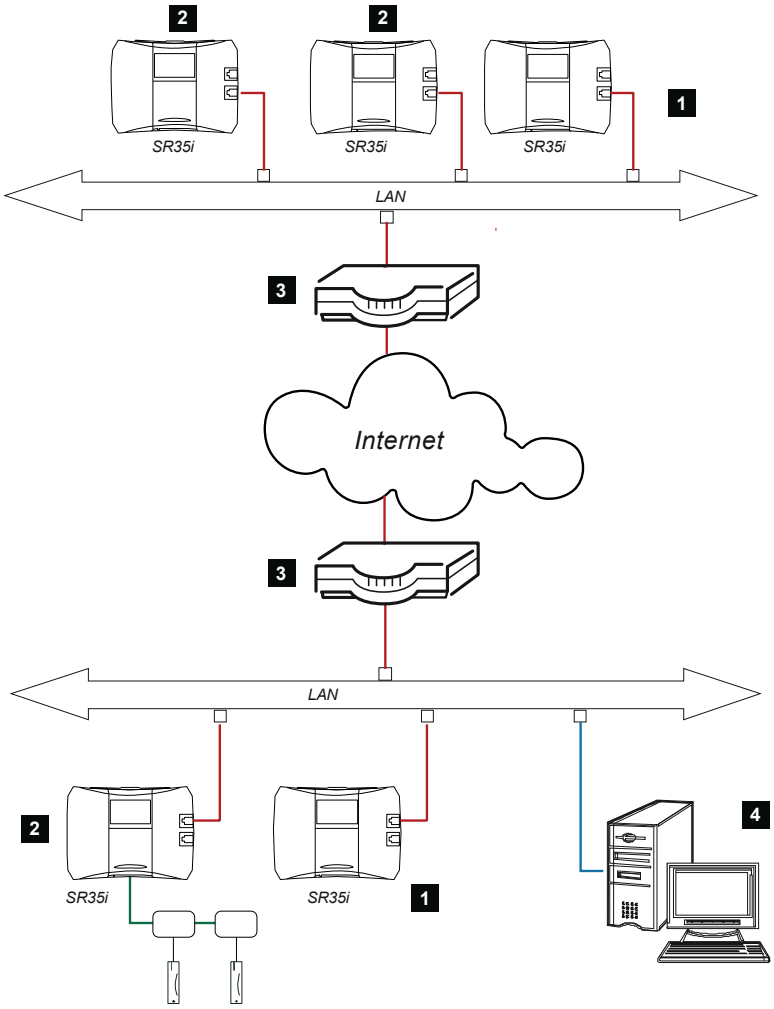
9.5 Firewall

In systems where a firewall is used and there exist external SiPass Entro equipment some actions will be needed.

Depending on the application some ports and IP addresses have to be opened. Consult the IT manager.

9.6 Example with router

In most cases the access control system is installed in local area network (LAN) where both dynamic IP addresses and “subnets” are used. The diagram shows an example using internet.



Internet solution with routers

1.	SR35i acting as a subnet agent. This SR35i will get a dedicated “fixed” IP address and is ported in the router (item 3). The subnet agent manages the communication to any of the other SR35i (items 2) on the same subnet.
2.	SR35i that resides “inside” subnet and have a dynamic IP address. But can not directly be reached from outside the router.
3.	The routers must be setup with the correct port and IP address to the subnet agent.
4.	Administration PC

9.7 Apartment building – example

We assume that an apartment organization shall install a new SiPass Entro system in three different houses, where we use three SR35is. We now describe how the controllers are configured with DHCP and we use DynDNS because the ISP does not allow static IP addresses.

A laundry room also exists in one of the buildings where the SiPass Entro **reservation system** shall be used, the tenants will use their home PC to make bookings and get confirmations.

The requirements for this are:

- A LAN must exist in each building where SR35i is installed.
- An Internet account must be available to allow for identities for the SR35is.
- One SR35i must also have the CF8 flash memory installed for reservation functions.
- The final system will have an administration PC installed.

The three controllers can be prepared in advance (before mounting) because they include a battery keeping the information (database) until the final installation is done.

Follow these steps:

1. Sign up for a DynDNS account [→ 52] with domain name **dynalias.net**, User name **MyAccount** and the password **MyPassword.**
2. Apply these settings to the SR35i:

SR35i	Name (in log)	Network ID
1	Controller House 1	house1.dynalias.net
2	Controller House 2	house2.dynalias.net
3	Controller House 3	house3.dynalias.net

1. Install the software [→ 55] in the PC. Enter House1.dyndns.net as network ID for the first controller (that the PC will use for communication).
2. Select the alternative to report to **DynDNS.org** and enter the Account type Dynamic DNS, User name MyAccount and password MyPassword and exit.
3. Configure all SR35i manually with the **New** button and enter name etc.
4. Proceed with the tab **Network** and mark the tick-box **Obtain an IP address** automatically (also the DNS address can then be allotted).
5. Enter the **Identity** according to the above table. I e House1.dynalias.net etc. Simultaneously you enter the name of the ISPs e-mail server (e g mail1.telia.com) to prepare the controller to send confirmations.
6. Set up all SR35i in the same way.

10 Installing the software

After the software installation (from CD) you shall open the Installer application.

If the system will use dynamic IP addressing technique (DHCP) on the local area network – you should prepare the network [→ 49] resources before installing.

Normally the installation automatically starts when the CD is loaded. Otherwise proceed like this:

1. Go to the **Windows** > **Start menu** > **Control panel**.
2. Double click the **Add/Remove Programs** icon.
3. Click **Install**.
4. Insert the CD in the CD ROM drive and click **Next**.

⇨ Follow the instructions on the screen.

Dependent if the system is new or not, different steps are performed to achieve the final solution. E g if it is the 1st or 2nd PC, exchange of PC, expansion with more SR35i etc, the Installer program is used in different ways.

Sometimes you have to know the system name as well as the user name & password to be able to use the software.

We use a wizard to create the initial communication link to a SR35i controller.

10.1 Creating a basic database and connection

The first time you open the Installer application there is no database or information about any **connection** to use in the PC. Therefore a wizard starts requesting the necessary parameters. Depending of the selections made some of them might not be needed.

Default is that one computer is connected and the tab Connections is not visible in the Installer application.

If more than one computer shall be used, please read the section Multi-user environment (more PCs) [→ 58] .

Proceed like this:

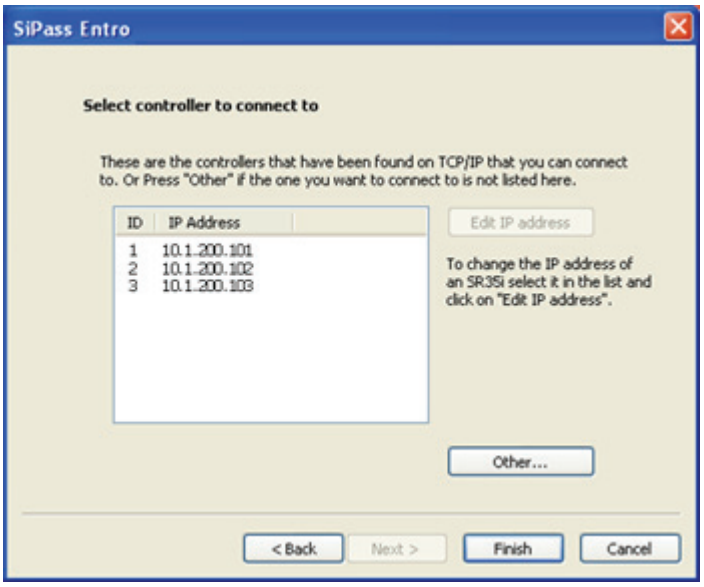
1. Go to the **Windows** > **Start** menu
2. Choose **Programs** > SiPass Entro> **Installer**.

   ⇨ The wizard starts.
3. Select **new** or **existing** system:

   – **New:**
   No system is configured yet and requires a **Site name** and a **System name**. (The crypto key, user name and password are known at this stage).
   – **Existing:**
   There is an installed SiPass Entro to connect. The **system name, crypto key** must be known as well as the **user name** and **password** that system.

4. By default the wizard searches on the local area network and the serial port for any connected SR35i and displays a list of segment controllers found. Also controllers connected to a COM-port in the PC will be found.

⇨


SiPass Entro
Select controller to connect to
These are the controllers that have been found on TCP/IP that you can connect to. Or Press "Other" if the one you want to connect to is not listed here.
ID
IP Address
1 10.1.200.101
2 10.1.200.102
3 10.1.200.103
Edit IP address
To change the IP address of an SR35i select it in the list and click on "Edit IP address".
Other...
< Back
Next >
Finish
Cancel

5. From the list, you select the SR35i you intend to use for connecting to this PC. Note - only one can be used!

6. **Finish**.

Manually decide on SR35i

If the correct SR35i is **NOT** found in the list, this indicates that the intended controller is located outside the local network and its IP-address has to be configured manually. The network [→ 49] must also be configured correctly to get the PC online.

1. Select how this PC should communicate with the site (**TCP/IP**, **RS232** or **modem**)?
   - If you select **modem**, enter the telephone number to the SR35i modem. Proceed by clicking **Finish**
   - In case of **RS232** the software automatically detects the correct COM-port in the PC. Proceed by clicking **Finish**.
   - If you select **TCP/IP** the wizard needs more parameters. Proceed by clicking **Next**.
2. Select **Static IP** or **dynamic IP address** (DHCP).
   - Enter the IP address of the SR35i to connect to if static is chosen.
   - If dynamic IP is to be used, follow the instructions on the screen. Note that the SR35i component [→ 90] needs to be properly configured. The built-in keyboard and display can be used.
3. Click **Finish** and the Installer main window are displayed.

	⚠ **CAUTION**

	It is very important that you make a note of the system name If you have to replace the PC this system name must be entered before the system will work again

Normally you will now see detected units where you then select either to configure all units or at least one SR35i (according to the section Automatic detection of units)

You should now wait until both indicators are green [→ 77] before continuing.

As long as you are still in the Installer program the events will be displayed in the Door monitor application (if started).

10.1.1 Automatic detection of units

The Installer program has embedded functions for “finding” addressed and connected segment controllers and door centrals. Subsequent expansions with additional units will also be found in then same way.

If the site is correctly installed, with appropriate addresses, you only need to step through each SR35i and door centrals. A list of units will be displayed on the screen as soon as login to Installer is done. A SR35i is displayed as **Cxx and a door unit or IOR6 is displayed as **Cxx:Dyy.

10.2 Multi-user environment (more PCs)

If only one computer will be used, no special arrangements are needed. A connection has been created automatically by the installation wizard. In cases where several computers shall be connected the software must be setup for using more than one **connection**.

Every PC (used in network applications) should be linked (connected) to the same SR35i. This is especially important if a SR35i is used as a “subnet agent”. Any controller that is managed by this subnet agent cannot be linked to any PC.

Proceed like this:

▷ Every PC must have a valid SiPass Entro software license.

1. Go to the **Connection** tab in the **System/System settings** and select that several computers can be connected concurrently.
2. Click **OK** – and a new tab appears in the main window in the Installer. The default, earlier hidden connection is now displayed as #1. Change the name of it before going further.

To get the Segment Controller to store events you have to **create a correct connection for each computer**. When this is done the SR35i will know, any time you logon, which PC to receive and store events from.

Proceed as follows:

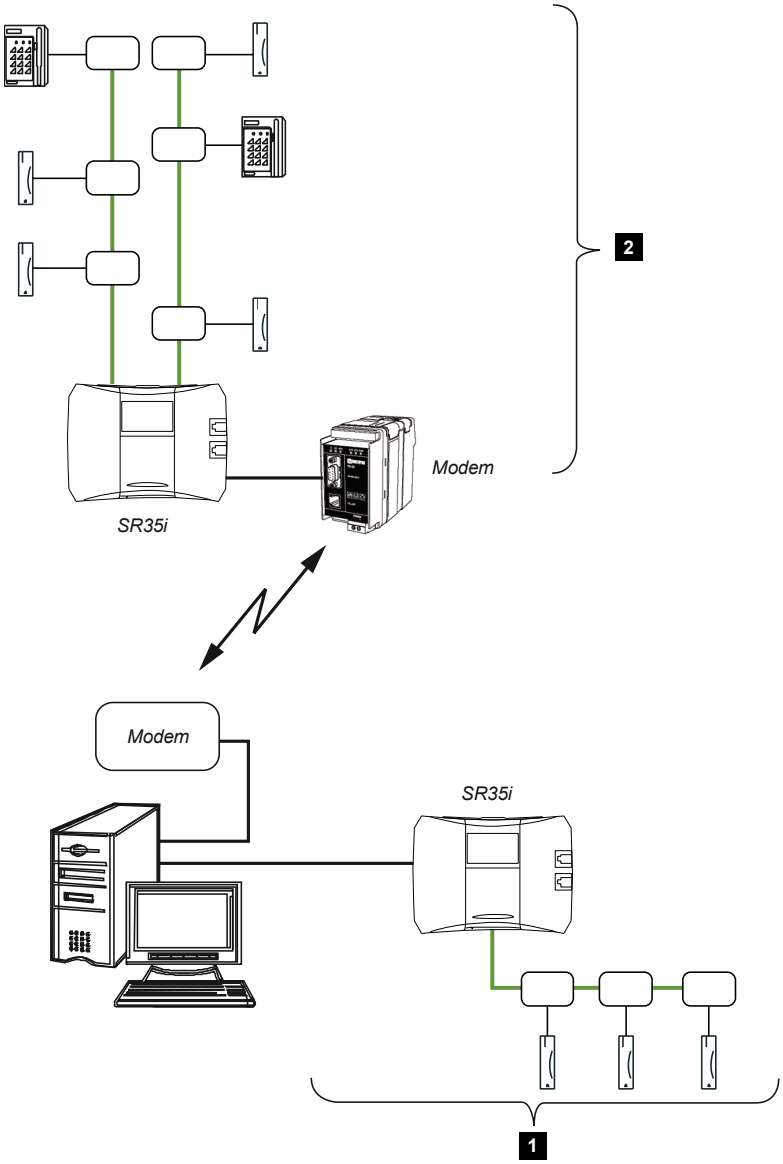
1. Go to the tab **Connections** (in the Installer program) and click **New**.
2. A wizard starts and you select SiPass Entro – System administration – and click Next
3. Enter a name of the connection, which **SR35i**, which **license number** and the **communication method**.
4. Finish.
5. Repeat for every computer to be connected.
   You have now created correct connections between PCs and the SiPass Entro system.
6. Proceed to make all the necessary settings for the installed SiPass Entro units.

We also recommend that you also create System Users to be able to manage the event filters, storing places and automatic logoff in a more flexible way.

11 Installing modem based systems

Up to 10 000 SiPass Entro systems may be controlled from one PC. If several systems are to be connected **directly** to a PC, the PC must have as many COM ports as there are SiPass Entro systems. PCs communicating with one system directly and with another via modem must have one COM port for connection of a segment controller and another for connection of a modem.

Below is an example of a configuration where a PC has direct contact with one SiPass Entro system and modem contact with another.



Example of a modem based system managed from a PC (in combination with a wired system)

1.	System #1
2.	System #2

11.1 Configuring a system equipped with TD36 modem (recommended)

We strongly recommend using the TD36 at the site when using modem communication because it has e g a watch-dog.

If you have installed a modem TD36 at the remote site (and its telephone number is available) there is no need to do the configuring on site. You can connect the SR35i to the modem, hook on the line but do the configuring at the host computer instead (even if this may take longer time). See more about transferring the new system's information to the central PC [→ 63] .

However – if you still want to configure it on site, you do this through the RS232 link and then switch to modem when it is done. Proceed according to the section Configuring the modem based system on site [→ 60] .

11.2 Configuring a system equipped with a custom modem

If another modem (not TD36) is used there may be a need of changing the init string of the modem and configured on site (via RS232).

You should then, temporarily, connect a PC with the SiPass Entro software to one of the segment controllers to be able to configure the system (see the next section Configuring the modem based system on site [→ 60]). When the configuring is finished you can disconnect the PC and connect the modem instead.

Do not forget to test the communications [→ 74] circuit and the power supply [→ 74] .

11.3 Configuring the modem based system on site

Configuring the new system should be done on location, i.e. with the PC connected (with RS232) to a segment controller in the new system.

1. Open the Installer [→ 76] application.
2. Click the tab **New connection** and you start a wizard to establish the connection between the PC and the controller. No login is needed because the system (database) is probably new and will use the default user name bewa and password pass.
3. Select **New system** and proceed.
4. Select **RS232** and proceed.
   ⇨ The software automatically detects the correct COM-port.
5. Enter a name for the new system in the **Site name** field, e.g. Oak lane.
   ⇨ This name will be displayed in the SiPass Entro Login windows, for the user to choose whichever system he or she wants to work with.
6. Enter the system's name in the **System name** field. This name must be **unique and identical** with the name you will be asked to enter when setting up the main computer (see Transferring the new system's information to the central PC [→ 63]).
   It is **very important** that you make note of the system name. If the PC has to be replaced you must enter the same system name once again.

7. Exit the wizard by clicking **Finish**.

   ⇨ Now the Installers main window is displayed.

8. You perform the set up of doors etc when you are on site according to the instructions given in the User manual. (Instead of later on via the modem connection).

   ⇨ Now the main configuring is done and you now prepare to connect the modem.

9. In Installer click on the **Connection** tab.

10. Mark the tick box Modem and a new tab is displayed.

11. Enter the **modem telephone number**.

12. A suggestion for the modem's so called init string is automatically displayed in the **Init string for SR35i modem** field. This string means "command echo disabled", "auto answer off", and "DTR disconnected". The string can be modified if needed.

13. If the modem needs to be able to call the PC, enter the desired telephone number in the **Telephone number to PC** field.

14. If the modem needs to be able to call the PC, you enter the name of the **System user** who shall dial up the PC (so that the PC knows where to store the events). Set also for which circumstances. The following alternatives exist:

    - After (desired number) events. Means that the segment controller calls the PC following the desired number of events.
    - On every event set to alarm. Means that the segment controller calls the PC following each alarm event.
    - On database changes. Means that the segment controller calls the PC following each modification in the database. This only applies if another PC is connected to any of the new system's segment controllers. A call is made every 15 minutes if the database is modified.

15. Click **OK**.

    ⇨ Now you have configured all the information about the new system.

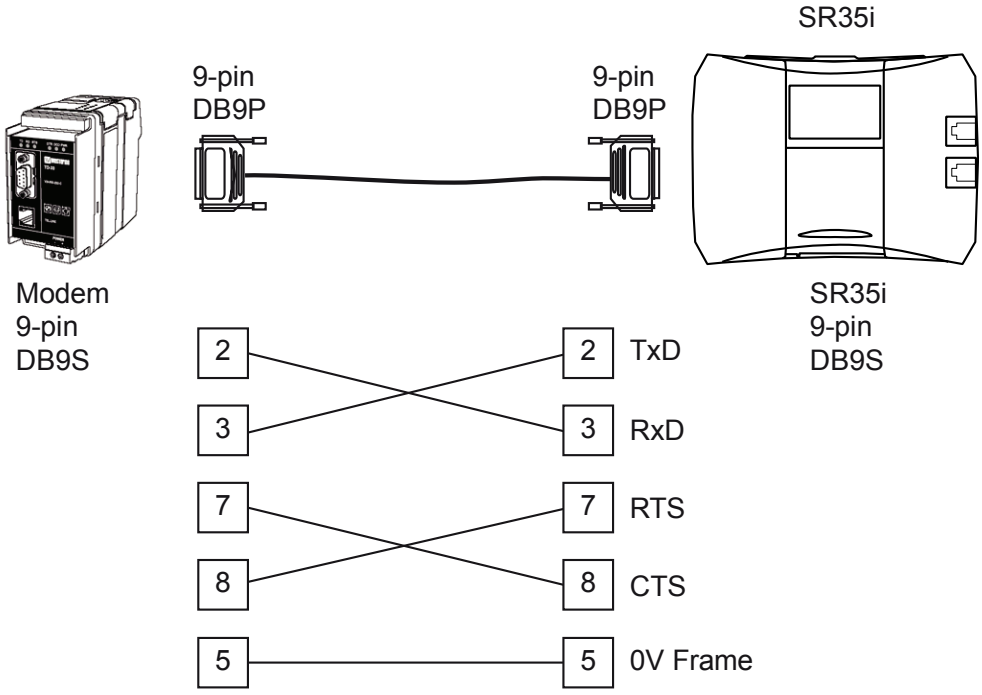
16. Disconnect the PC you have used for configuring the system and connect the modem [→ 62] instead

Activation and deactivation of alarms as well as PIN alterations are a database modification, which means that calls will be made every time this occurs.

Entroser must be running in the PC to be able to receive calls about database modifications

11.4 Mount and configure the modem

The illustration below shows how to connect a modem to the segment controller used for communication with the PC.



When the modem is installed the installation is completed. The only thing remaining is to transfer the information configured for the new system to the central PC used to configure both systems.

Minimum requirements for modem:

- 9600 bit/s
- Auto answer off
- DTR disconnected
- Command echo disabled

Recommendation:

The modem should have Watchdog built-in. Watchdog resets the modem automatically in case of an interrupted connection or power failure.

If the modem runs on 12-24V, it can be powered by the system's supply, in which case it will also make use of the system's battery backup.

11.5 Transferring the new system's information to the central PC

Go to the PC to be used for configuring and monitoring both systems.

If this PC has not the SiPass Entro installed, install it from the CD.

Then you will need to **create an initial connection** in the PC (to the modem) to be able to transfer the information. Later on you only have to select which system/connection, login and dial up as usual.

1. Open the Installer [→ 76] application
   ⇨ Note that if the PC has no system installed, the wizard starts automatically and you start the wizard directly (without login).
2. Go to tab **New connection** and start the wizard.
3. Select **Existing system** and proceed.
4. Mark the modem choice and enter the telephone number of the modem.
   ⇨ Now the connection is set up and you might continue dialling up the remote site as below - or later you can log in and dial up.
5. Enter the **Site name** and **System name**.
   It is very important that you enter the same system name as when you installed the modem. If the PC has to be replaced you must enter the same system name once again.
6. Exit.
   ⇨ The wizard will now try to connect (dial-up) the remote site. If this fails – proceed as below.
7. The SiPass Entro Installer main window is displayed. The name of the chosen system is displayed in the window's title bar. Since you have not yet called the new system you are OFF-LINE.
8. Click the lifted handset symbol on the tool bar or choose **Call** on the **Modem** menu. A message is displayed while the system tries to establish a connection.

When the connection is established the systems are in direct contact, i.e. the green ON-LINE [→ 77] indicator is lit. When all information is transferred (this may take a couple of minutes) the DB UP TO DATE [→ 77] indicator will also turn green.

The new system is now ready to receive information about time schedules, persons, access groups and doors.

SiPass Entro should always be ONLINE (connected via modem) when configuring a modem-controlled system. This way information transfer will be quicker and safer.

12 Installing the CF8 flash memory card

The CF8 memory acts similar to a hard disk unit for storing files. When delivered it contains the HTML-files used in the Reservation system.

1. Remove the power from the actual SR35i.
2. Install the CF8 card.
3. Reconnect the power to the SR35i.

When all other necessary parameters and units for Reservation are configured, you can connect to the IP-address of the SR35i (http//xxx.xxx.xxx.xxx./login.html) – and the login page should be displayed.

13 Install DVRs

SiPass Entro has integrated functions for controlling an external DVR system in the Siemens SISTORE™ range. There are different capacity and settings depending of which DVR product that is used.

This describes which parameters to set in the different SISTORE™ models and which additionally cautions to consider getting them work in the SiPass Entro environment.

For all models - it is recommended to print the documentation on the CD (supplied with the DVR) before any configuration is done.

13.1 Prerequisites

We assume that the DVR system is installed and documented according to its handbooks and that the DVR have been configured for communication with the SiPass Entro system. E g must the LAN environment allow for communication between the units.

Normally there is an user interface (PC software) for the DVR-system meaning that initial settings are done with this software – or in some units basically by means of the front panel in the DVR.

!	*NOTICE*
	Always calculate on the number of cameras used, frame rates, resolutions and the size of hard disks that are available in the DVRs before configuring any triggered or continuous recording commands in the application. Otherwise there might be a risk for data loss when the recording memory ends.

DVR Viewer

You should also have installed the Viewer software that fits the actual DVR models. Several can exist concurrently in the PC.

Obviously if **not** installed, the SiPass Entro can not display any images from the particular DVR in use. (The SiPass Entro will notify the User to install the software).

Normally the Viewer software is supplied with the DVR. If not – contact your SISTORE™ supplier.

Clock synchronizing

Both SiPass Entro and the DVR have their own calendar clock functions. These should be synchronized to guarantee that events and images get the same time stamp.

The best solution is to let both systems update their clock from the same source (usually an NTP server). Also the SR35i can act as a server for the different SISTORE™ recording systems.

The SR35i Segment Controller can be setup according to this. See the section Advanced system clock management [→ 80] .

The DVR is setup according to its handbook.

13.2 DVR connection

When the SISTORE™ DVR is installed and configured, some parameters in SiPass Entro software must be configured to be able to communicate with the DVR at all.

The communication between the DVR and SiPass Entro is done via a TCP/IP link. In the SiPass Entro a “connection” must be created for each DVR.

In a single-PC based system, the tab Connections will not be visible directly. You have to go to the tab **System > Systems settings > Connections** and configure the SiPass Entro to work with several connections (like a DVR).

Proceed like this:

1. Open the Installer [→ 76] application.
2. Click the tab **Connections** If not visible – see the note above.
3. Click **New** – and select **SISTORE DVR** in the wizard.
4. Enter the suitable **Name** of the DVR.
5. Select which **SR35i** to use.
6. In the list box choose **DVR type**. This choice will implicitly also configure the SiPass Entro database to use the **default network ports** in the DVR.
7. Enter the selected **User name** & **Password.**
8. Click **OK**.
9. Repeat the above for each DVR.

13.3 How to control recordings?

There are different ways to start recordings from the SiPass Entro

- Event triggered during time zones.
- Continuously recording by time zones.
- Manually recording (started from the Door and event monitor application).

Event triggered during time zones

Different event triggers in SiPass Entro can result in an automatic recording and storing of images in the DVR unit (no recordings are stored in the PC).

E g can a door alert start a recording during night time only by creating a suitable SiPass Entro time schedule and tie a **time zone** e g *Other time* to the filter settings together with pre-and post recording times (= how long the recording lasts before and after the event).

Continuously recording by time zones

You can use a SiPass Entro time schedule to control a continuous recording from a camera but that may generate large files on the DVR.

13.4 Camera settings

As soon as a DVR has been configured in the Installer program there will be another tab “Cameras” where each camera must be configured. Proceed like this:

1. Go to the tab **Cameras** (in the Installer program).
   All cameras that are not configured in the database will be displayed as **<DVRNAME>:<CAMERAINDEX>. This might however take some time.
2. Select a camera and click **Edit**. Or click New for manually adding a camera.
3. Change the **Name** of the camera. The DVR that stores the images and the index number will normally be defined by software.
   However – if the camera were added manually these parameters must be set.
4. Select (or create) a **time schedule** for this camera. This could be any of the SiPass Entro time schedules.
5. Two main starting criteria can then be used.

By default the parameters configured in the DVR itself will be used for recordings. Typically the frame rate and resolution but also pre- and post recording time values.

Depending of the DVR in use, the SiPass Entro

software then has different capability to control parameters of the DVR. See the table below for details of where to set values.

Value to set	AX	MX	CX
Pre-recording value	Same in DVR and in SiPass Entro	In SiPass Entro	Only in DVR – See SISTORE CX [→ 72]

Value to set	AX	MX	CX
Post-recording value	In SiPass Entro	In SiPass Entro	Only in DVR – See SISTORE CX [→ 72]

1. If any **continuous** recording shall be used, choose which time zones to actually have the camera recording. Be very careful because this function can generate very large files on the DVR hard disc!
2. By **filtered triggering**. Click on the tabs Recording set 1 and/or Recording set 2 and do the following:
   - Select (or create) an event filter to trigger and start a camera recording. By default all event types, as well as doors, are disabled. Mark any events in the first tab and doors in the second tab.
   - Select during which times zones you want to monitor events (using the filter).
   - Configure different pre- and post recording times for each. Note that possibilities to change these can differ depending of the models used. In this way you can e g have one set with very short times and the other with longer.
3. Click **OK** and repeat for each camera.
4. If you want to change anything, just click Edit.

⇨ You have now made the settings needed to have images transferred from the DVR to SiPass Entro for viewing.

13.5 SISTORE™ MX

There are some initial steps to carry out via the SISTORE™ MX software before any SiPass Entro software can communicate.

Normally you probably install the whole MX software suite to be able to both control the detailed settings of the MX DVR - as well as viewing. It is however possible to only install the RemoteView module to view recordings from SiPass Entro.

We recommend that the MX software is installed on the C-drive.

13.5.1 MX Parameters

You must confirm (or re-configure) the use of and note down the following parameters in the MX type of DVR:

Parameter	Default value	Optional User Value:	Comment
User name:	Administrator		Entro parameter
Password:	Administrator		Entro parameter
IP address	<Not set>		**Entro parameter**
Port	40	N/A	<Fixed in Entro>
Port SR <-> DVR	8080	N/A	<Fixed in Entro>
Port range	1100 - 1109	N/A	<Fixed in Entro>
Camera no's and names	<Not set>		Entro parameter

It is a good idea to name the cameras equally in both the DVR and the SiPass Entro environment because otherwise it is a risk that the on-screen name differs from the name seen in the SiPass Entro event log.

When the parameters are configured – enter them into the SiPass Entro **Installer** application when creating connections and cameras.

13.5.2 MX Live Viewer software

If you only want to do the basic viewing from SiPass Entro, just install the RemoteView module on the actual PC where SiPass Entro is installed. Otherwise no view will be displayed

13.5.3 Additional considerations for the MX

Following settings must be performed in the MX:

- In the configuration "software trigger" has to be activated to start recording. You have to activate that at the MX itself. It's not possible with the remote configuration.
- Continuous recording has to be activated. This can also **only** be activated at the MX itself.

13.6 SISTORE™ AX

13.6.1 General

When integration the range of SISTORE™ AX DVR:s in SiPass Entro there are a couple of settings that has to be correct in the DVR in order for getting a correct functionality.

- Continuous recording setting in SiPass Entro causes problem from event recording and is recommended to not be used.
- Note that if you connect a VGA monitor to display the on-screen menus (and images) – check that the rear selector switch are set to VGA.
- VGA monitor output does not exist for every AX, it depends on the model.
- You also install the supplied **PC software** for remote control of the AX in the actual PC where SiPass Entro is installed. Otherwise no views will be displayed.
- Although you will see the AX Admin, AX Watch and AX Search software commands in the PC – you should be careful using them when the SiPass Entro application is running.
- In RAS v3.5 and above, the separate applications AX Admin, AX Watch, AX Search are integrated into one user interface. RAS v3.5 has higher requirements regarding system performance (please refer to DVR documentation). Previous RAS versions are not supported any longer.

13.6.2 AX9 and AX16

A schedule has to be created and in use with the following characteristics:

- Day: All
- Range: 00:00 - 24:00
- Mode: Event
- Channels: All connected cameras.

Make sure that "Schedule on" is activated in the "Recording" menu.

13.6.3 AX4 and AX Lite

- ‘Quick setup’ should be disabled.
- ‘Time-Lapse Recording’ must be set to "Off".

13.6.4 AX Parameters

You must confirm (or re-configure) the use of and note down the following parameters in the AX type of DVR.

It is possible to use the buttons on the AX front panel to configure the basic parameters (e g the IP parameters) according to the AX Quick start guide. As soon as you have established a LAN connection to the AX you can optionally configure the parameters from the PC.

Parameter	Default value	Optional User Value:	Comment
User name:	<Not set>		Entro parameter
Password:	12345678		Entro parameter
IP address	192.168.1.129		Entro parameter
Gateway	192.168.1.254.		Entro parameter
Subnet mask	255.255.255.0		Entro parameter
Port: SR <-> DVR	17655	N/A	<Fixed in Entro>
Port: Watch	8016	N/A	<Fixed in Entro>
Port: Admin	8200	N/A	<Fixed in Entro>
Port: Search	10016	N/A	<Fixed in Entro>
Port: Callback	8201	N/A	<Fixed in Entro>
Camera no's and names	<Not set>		Entro parameter

The table is valid for the following AX devices:

- SISTORE AX4 Lite
- SISTORE AX4 160/100
- SISTORE AX9/AX16 250/50

Since SISTORE AX9/AX16 250/200 has enhanced user authentication, a user name is mandatory for authentication with the device (same for future SISTORE AX8/AX16 250/100). A default account is set up on the device (user name "admin", no password).

It is a good idea to name the cameras equally in both the DVR and the SiPass Entro environment because otherwise it is a risk that the on-screen name differs from the name seen in the SiPass Entro event log.

13.6.5 Additional considerations for the AX

For AX4 Lite, AX4 160/100 and AX9/AX16 250/50, the following settings must be performed:

- No recording configuration in the time lapse recording setup
- At AX9/AX16 250/50, the REC button has to be activated on the AX device

For AX9/AX16 250/200, the following settings must be performed:

- In the Schedule screen the recording mode has to be set to Event

For AX16 the following settings must be performed:

- The record button has to be switched on
- In the network settings the “Transfer Control” has to be switched on

When the parameters are configured – enter them into the SiPass Entro Installer application when creating connections and cameras.

13.6.6 AX Live Viewer software

Note that only **one live view window at a time** can be displayed using the AX Watch remote software.

This means e g that if SiPass Entro is displaying a view in the Installer when setting up a camera you cannot concurrently view an image in the Door Monitor (by clicking on a camera icon).

In RAS v3.5 and above, the separate applications AX Admin, AX Watch, AX Search are integrated into one user interface.

13.7 SISTORE™ CX

13.7.1 General

The CX model uses PC software module for configuring and viewing. Read more in the Quick setup or the DVR Configuration manual.

We recommend that the SX-CX software is installed on the C-drive.

Note that the CX includes an integrated “homepage” which can be browsed for more information about the actual unit. As soon as the “device list” is configured it is possible to connect.

13.7.2 CX Parameters

The DVR does not have any front panel buttons to re-configure e g its network settings locally. Therefore it is recommended to initially use a PC with the SX-CX-Config software installed (without any other network connected) and connect the network cables only to the DVR.

As soon as the steps according to the DVR manual are done you then confirm (or re-configure) the use of and note down the following parameters in the CX type of DVR using the **SX-CX Config** program:

Parameter	Default value	Optional User Value:	Comment
User name:	admin		**Entro parameter**
Password:	admin		**Entro parameter**
IP address	169.254.16.9		**Entro parameter**
Subnet mask	255.255.0.0		**Entro parameter**
Gateway	0.0.0.0		**Entro parameter**
Port	12050	N/A	<Fixed in Entro>
Port SR <-> DVR	12050	N/A	<Fixed in Entro>
Camera no's and names	<Not set>		**Entro parameter**

It is a good idea to name the cameras equally in both the DVR and the SiPass Entro environment because otherwise it is a risk that the on-screen name differs from the name seen in the SiPass Entro event log.

When the parameters are configured – enter them into the SiPass Entro Installer application when creating connections and camera settings.

13.7.3 CX Live Viewer software

The software for remote viewing, currently named **SX-CX Client**, on the DVR must be installed in the actual PC where SiPass Entro is installed. Otherwise no view will be displayed.

13.7.4 Additional considerations for the CX

The IVM rules (standard) have to be activated to get the pre- and post-recording functionality in the DVR to work.

14 Before configuring the system

Before commissioning the SiPass Entro system, the installer should read and complete the checklist [→ 75] .

14.1 Check the communication circuits

Go to all units in the system and check that they are communicating.

When all units are connected (but with all removable **terminal blocks disconnected** in drop boxes and door controllers), check on reader block nos. 3 and 4 in drop boxes, door controllers and segment controllers that the resistance on the global and the local communication circuit respectively, is 60 Ω (ohm) plus the cable resistance.

- If the resistance is 120 Ω plus the cable resistance, one termination resistor is missing. If the resistance is much less than 60 Ω, there is a short circuit in the communications circuit.
- If the resistance is much greater than 120 Ω (open circuit), there is a break in the circuit or the termination is missing in both ends.

If using a LAN, check that all cables are correctly connected to the LAN.

14.2 Check the power supply

Connect the power supplies. Check that the voltage is approximately that of the power supply output and that + and – are in the right positions.

Remember that a voltage drop (between the highest and lowest potential) larger than 5V between units may influence the quality of the RS485 communication.

15 Checklist

The checklist below is a useful aid when installing SiPass Entro. It will also make sure the implementation will run smoothly. If you have questions, do not hesitate to contact technical support.

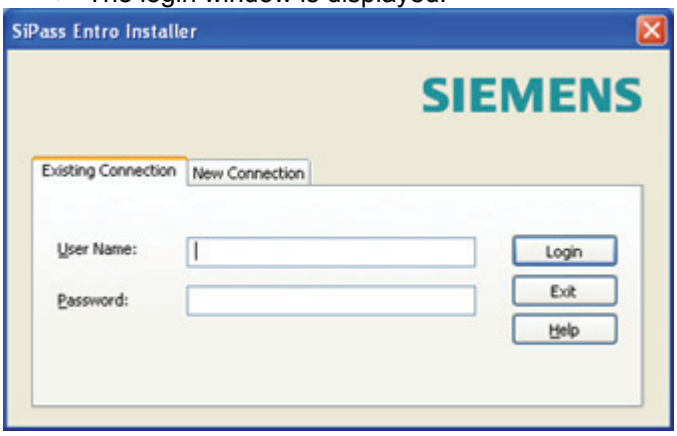
The operating system in the system's PC is:	❒ 2000 ❒ XP ❒ Vista ❒ Terminal server 2008 ❒ Terminal server 2003 ❒ Windows 7
If RS232 is to be used - are there free serial COM ports (9/25-pin plug) in the system's PC	❒ Yes
Is the wall socket (RS232) installed close to the system's PC and connected to a suitable SR35i and is the total distance between PC and SR35i less than 25 meters?	❒ Yes
If local area network is to be used – does the PC have a correct connection?	❒ Yes
Have the SR35i got correct IP-addresses – authorized by the IT-Manager?	❒ Yes
Have all networking resources (routers, firewall etc) the correct settings?	❒ Yes
Have all connected segment controllers, readers and door controller's proper addresses?	❒ Yes
Is the reader connected to correct terminal block in DC22/DC12 and is the power link correctly fitted?	❒ Yes
Is a 120-ohm resistor fitted at the end of each RS485 communication circuit?	❒ Yes
Does the resistance in all communication circuits comply with the values recommended in the manual?	❒ Yes
Is each circuit's screen connected to earth in one place only?	❒ Yes
Are the power supply equipment and cables properly dimensioned?	❒ Yes
When Reservation is used – is at least one CF8 installed in a SR35i	❒ Yes
Is time and date properly set when the system is on-line	❒ Yes
Is any installed DVR properly configured?	❒ Yes

16 Start the software

The first time you start the SiPass Entro software you will be requested to create a system user and thereafter logon again to be able to store events.

1. In the Windows start menu, select **Start** > **Program** > SiPass Entro.
2. Choose one of the three applications: **Installer**, **Entro** or **Door Monitor**.

   ⇨ The login window is displayed.



3. Enter the user name in the **user name** field (default: bewa).
4. Enter in password the **password** field (default: pass).
5. If several systems exist, select one system.

   ⇨ If more than 20 systems exist there will be an additional search field.
6. Enter a character.

   ⇨ The system finds any name that includes this.
7. Click **OK**.

⇨ The SiPass Entro main window is displayed.

Start applications via the icons

It is possible so quickly start an Entro application, by using the icon. Proceed like this:

1. Position the cursor over the icons and right-click.

   ⇨ A menu is displayed
2. Select SiPass Entro or Door Monitor

⇨ Either of the applications is started.

⇨ Note that the Installer application must be started via Windows start.

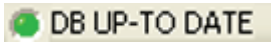
16.1 Indicators for communication status

Indicators in the application windows

In the bottom right of the box there are two indicators:

If the text ON LINE and a green indicator are displayed, the PC and the SiPass Entro application are connected to the access control system.

If the text OFF LINE and a red indicator are displayed, SiPass Entro has no contact with readers and controllers. This means that the information registered in the PC does not reach the segment controllers.



If the text DB UP TO DATE (DB = database) and a green indicator are displayed, the segment controller connected to the actual PC, have the same information as the PC.

Note that in some circumstances (like upgrading, larger import of persons etc) there could be a delay in the transferring of information from the “first” controller to the next. Please study the display information in each SR35i for the correct status information.

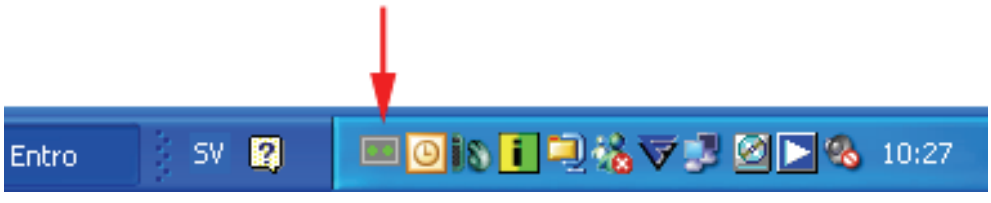
If the text DB OUT OF DATE and a red indicator are displayed, the segment controllers do not have the same information as the PC. Note that a certain amount of time may pass before the information has reached all segment controllers and that the system has to be ON LINE for this to be possible.

You can also look at the status bar to see how far the transferring of data to the PC has gone. Normally it might be events that are transferred (in cases where the PC has been OFF-LINE)

The default setting is that you will automatically be logged out of the system if no task is performed within 15 minutes. In the Entro application you may set the desired number of minutes or disable.

Indicators in the Microsoft Windows toolbar

In the bottom right of the window task bar the following symbol is displayed:



Entro icon in the Windows notification area

When displayed, an application called Entroser (SiPass Entro serial communication) is running in the background. This is a required condition for events to be displayed on the PC's screen and/or stored on hard disk. Entroser will be running even if you exit any SiPass Entro application.

Despite the name Entroser, this is also used in TCP/IP communication.

Close application and stop communication

In some cases a complete shut down of the SiPass Entro is required. E g during maintenance actions like updates, or similar. Proceed like this:

1. Position the cursor over the icons and right-click.
   ⇨ A menu is displayed.
2. Select **Close Entro**.

⇨ All communication (entroser) is stopped and the current database is stored. The icons disappear from the task bar. No events will be stored.

For **Windows 7**, to see the notification icon, **right-click in the notification area** and select **Customize notification icons**. Find the entry for Entro and choose to **Show icon and notifications** in the drop-down list.

17 Set time and date

Before starting to configure you should set the correct time and date. The clock is shown separately in the lower, right corner of the window.

Note that if any SR35i is set to TCP/IP and will get the time from an external SNTP timeserver – you cannot manually set the clock. See section Advanced system clock management [→ 80] .

Proceed as follows, if the system lets you correct the system clock:

1. Check that the indicators in the lower right corner of the windows SiPass Entro display ONLINE and DB UP TO DATE.
2. Open the Installer or Entro [→ 76] application.
3. Choose in the menu **System > Entro system clock**.
4. Check that the correct date and time are displayed. If not, enter the current date and time in the **New date** and **New time** fields.
5. To disable automatic daylight saving time changes, remove the tick next to the **Automatically adjust clock for daylight saving changes** prompt.
6. Click **OK**.

18 Advanced system clock management

You only have to make the steps below if you intend to let the SiPass Entro fetch its time externally and additionally allow each SR35i to adjust its time relatively to GMT.

SiPass Entro uses a Simple Network Time Protocol (SNTP) – which fetches an **international clock (GMT)** from an external SNTP process running on an external server – (on the LAN/Internet) – or an internal server (SR35i). SNTP is necessary for SR35i's that are network connected (TCP/IP). If in doubt, consult the IT manager.

If any network is used, the SR35i must be able to get the clock from a clock server – when TCP/IP is used. Every controller set to **Proxy** must also have this setting. This guarantees correct time in the system independent of where a SR35i is installed.

When you configure a SR35i as Proxy, it will need to know where to fetch the clock from. You can select internal or external. However - if running the SiPass Entro system in **multiple sub-networks** with Internet connectivity between, it's recommended to use an external time server.

If the clock server function resides in another subnet, the port 123 must be open in the router.

In the menu **System > Entro System time** in Installer program are more choices for the system clock. Do like this:

1. Check that the indicators in the lower right corner of the SiPass Entro windows display ONLINE and DB UP TO DATE [→ 77] .
2. Click **Advanced**.
3. Select method for time server:
   - Internal time server (e g SR35i) and select controller.
   - External time server (e g via Internet) and enter IP-address.
4. Select if every SR35i is allowed to correct its time relatively to GMT time.
5. If this is selected – every segment controller will display a new tab **Time** where the adjustment value is chosen (e g +1, +2 etc).
6. Exit.
7. Check in the menu **System > Entro System time** and check the choice of **Automatic daylight saving time changes**.

19 Personalize Entro settings

19.1 Card reader parameters

If cards other than SiPass Entro cards are to be used and if they will be read differently, you must change the card reader parameters.

1. Open the Installer [→ 76] application.
2. Choose on the menu **System > System settings**.
3. Click the **Card reader parameters** tab.
4. Enter the type of access cards to be used in the system.
   - SiPass Entro standard means that the system reads track 2 ISO format and positions 9-16 on the magnetic strip, or the last 8 positions if fewer than 16. (Standard SiPass Entro cards are encoded like this).
   - If other cards are to be used and will be read differently, click Custom. Then enter from which digit position on the magnetic strip data should be read and how many digits should be read (16 at the most). Some older readers maybe only read 8 digits. You should consult with Siemens Building Technologies if you are in any doubt about this.
5. Select in which way the digits shall be presented in SiPass Entro.

19.2 Personal code without card

Generally, PIN is used together with a card – during the Card + PIN security level. However, SiPass Entro offers each user the possibility of choosing a PIN instead of a personal card. Note however that activating this function disables Group code.

This is how to activate the function:

1. Open the Installer [→ 76] application,
2. Choose in the menu **System > System settings**.
3. Click the **Personal Code** tab.
4. Choose the Use of personal code without cards alternative.
5. Enter the desired number of digits to be used (4-8) in the PIN. Any user-choosing PIN without card must choose a code consisting of the number of digits chosen here.
6. Click **OK**.

19.3 Changing red LED function on readers

By default, the red LED is used to indicate an active alarm zone and will be lit on readers those are members of an alarm zone, once the alarm system is armed.

To disable this function and use the red LED for door locked indication, please proceed as follows:

1. Open the Installer [→ 76] application,
2. Choose in the menu **System > System settings**.
3. Click on the **Reader red LED** tab.
4. Check the box Use red LED for door locked indication.
5. Click **OK**.

This setting affects all readers on the system that are using BCLINK or RS485 connection (i.e. not Clock & Data readers). If this is checked it will not be possible to monitor alarm system status. We recommend not checking it if alarm zones are used

19.4 Duress code on/off

With the Duress function activated, a person entering the building is able to enter a specific code if forced to open the door under threat. Doing so, an alarm signal is sent to a connected alarm transmitter. When SiPass Entro is delivered the duress function is deactivated.

This is how to activate the function:

1. Open the Entro [→ 76] application.
2. Choose on the menu **System** > **System settings**.
3. Mark the **Enable duress** option.
   ⇨ A warning message is displayed.
4. Click **Yes** to activate the duress function.

20 Configure names for segment controllers

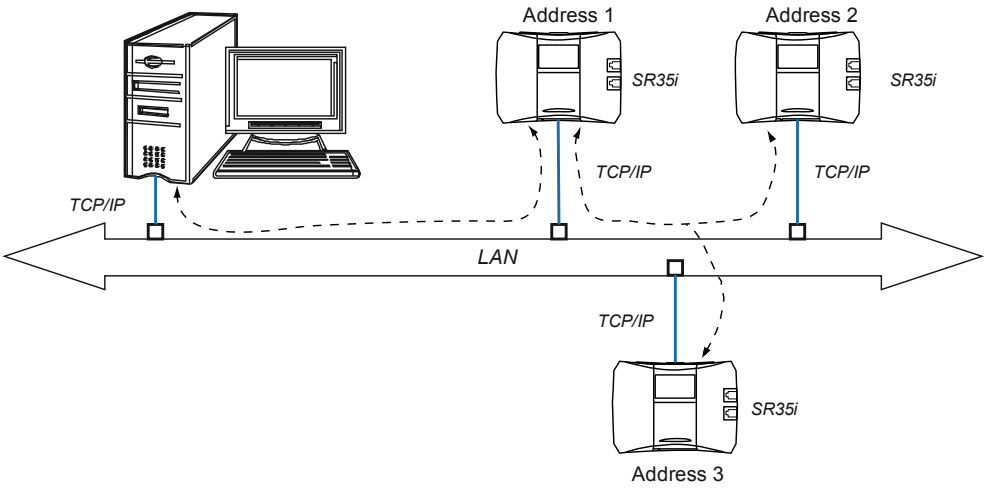
Dependent on how the SR35i's should communicate with each other, the parameters are set-up in different ways.

Remember that the basic parameters (like the IP address) initially can be set by using the integrated keypad in each SR35i. This means that you fulfil the requirements for communicating with the PC, but configure the rest of the settings in the Installer application.

If you intend to use dynamic IP addressing for segment controllers you should read more about preparing network [→ 49] .

If a modem will be used – please refer to the section Installing modem based systems [→ 59] for more information.

20.1 Create multiple SR35i for TCP/IP communication



In this case three methods can be used to set-up the SR35i segment controllers.

Configuring via RS232

A PC is connected to every SR35i via RS232 connection. The information is transferred directly into every SR35i.

RS232 is the easiest method to use, when the segment controllers are placed in different geographical areas. It is important that these get the correct IP-address, system name and encryption key.

Every new SR35i is displayed as **Cxx. Now proceed according to the steps in the section SR35i Configuring [→ 86] , to set the **IP-address**, **Proxy** and other necessary parameters.

Configuring via TCP/IP

In this case the PC communicates with a dedicated SR35i whilst the other controllers will get the information from this one (via TCP/IP). If the system is new, you will already have had the opportunity to configure the correct **IP-address**.

In the Installer program, the first SR35i is shown. If there are more non-configured SR35i they will normally "pop-up" on the screen (and be available for use in the actual system). Otherwise you have to use the command **New** to create the rest of

the controllers and to set the **IP-address**, **Proxy** and other necessary parameters according to the steps the section SR35i Configuring [→ 86]

Transferring the data to/from completely new SR35i will take some minutes (due to the load on the network). This also applies for updating the Door monitor program

Configuring via the keypad in the SR35i

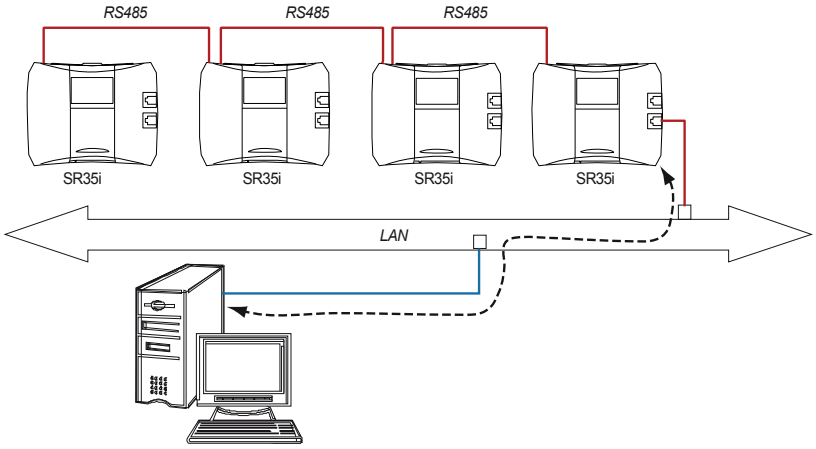
In some case it is not possible to connect to the SR35i from the PC. E.g. in a remote site environment. Instead the menu system in the SR35i can be used to configure the network settings. There is a built-in keypad and display which enables also for entering letters. Ensure that the settings are aligned with the setting in the PC software (database). See section SR35i Configuring [→ 86] .

20.2 Create multiple SR35i for combined TCP/IP & RS485 communication

The combination of a local network and RS485 requires that the controller used for TCP/IP has to be set-up as in the earlier section.

All other SR35i, using RS485, will be displayed with temporary symbols (**C1, **C2 etc.). The number refers to the segment controller's address.

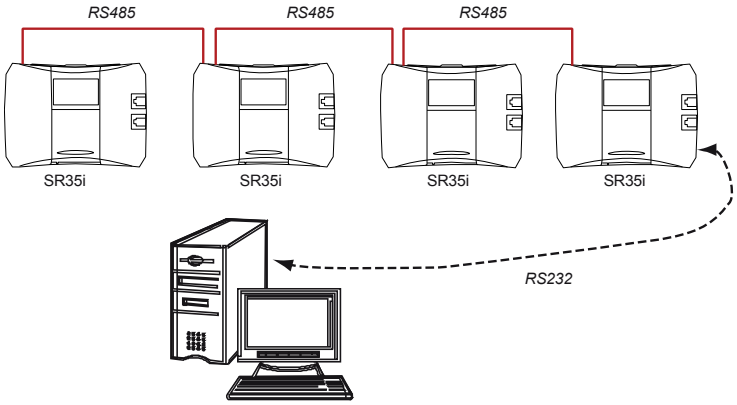
Then proceed with the steps in the section SR35i Configuring [→ 86] .



20.3 Create multiple SR35i for only RS485 communication

Systems intended for RS485 (no local network) – are configured via direct cable RS232. In this case all controllers will be displayed as **C1, **C2 etc – where the digit corresponds to the address jumper.

Then proceed with the steps in the section SR35i Configuring [→ 86] .



21 SR35i Configuring

In a new TCP/IP based system, you will (when invoking the Installer program) have the opportunity to add more not yet configured SR35i that the software "finds" on the LAN. You will see them in a list. Just select any one of them to be included.

1. Open the Installer [→ 76] application.
2. Select the desired segment controller (if it is not already selected) and click **Edit**.
   - Tip – You can also right-click and choose New, Edit or Deleted.
3. In the **Name** field, enter the segment controller's name. A suitable name is the room where the controller will be placed, e.g. Reception. Avoid using names that may later be confused with door names.
4. Mark the tick-box **Proxy** for SR35i using TCP/IP. If RS485 is used between all SR35is – but PC connection uses TCP/IP – the only need for proxy in the SR35i is for reaching an SNTP Time server. If there is a mix of RS485 and TCP/IP – the segment controllers using TCP/IP must have Proxy function.
5. Decide if the SR35i also should act as a subnet agent [→ 50] (similar to a gateway for other SR35i controllers "behind" a router).
6. Select the Network settings tab and enter the **IP-address**, **Netmask** and **Gateway**.
   - When powering-up the controller – the IP-address will initially be **10.1.200.1xx** (where xx indicates how the address is set in the controller) – or the one stated initially when locally setting up SR35i.
     Enter the **Netmask**, which can filter the addresses for messaging on the LAN. Often the value 255.255.255.0 can be used. Enter the address for **Gateway** (if one exists.) This can be used to take care of rejected addresses (filtered by the Netmask). Enter the IP-address for any Domain Name Server if e-mail functions are to be used.
   - Optionally both the IP settings (DHCP) and the DNS server address can be obtained automatically by clicking the check-boxes respectively. Note that the DynDNS functionally must also be setup in the software as well as in the SR35i.
7. Enter the actual **mail server** (SMTP) used in e g the Reservation system.
8. Enter the network identity for the segment controller.
9. Click on the tab **Time** (if displayed) and enter a **correction value** (+1, +2, -1, -2 etc). This should correspond to the geographical time zone where SR35i is installed. (Compare with GMT-time and the setting in an ordinary PC. I e +0 for Great Britain, +1 for Sweden and +2 for Finland).
10. Click **OK** and continue with the next segment controller until all the segment controllers on the system have been named.

21.1 Decide on network settings for SR35i

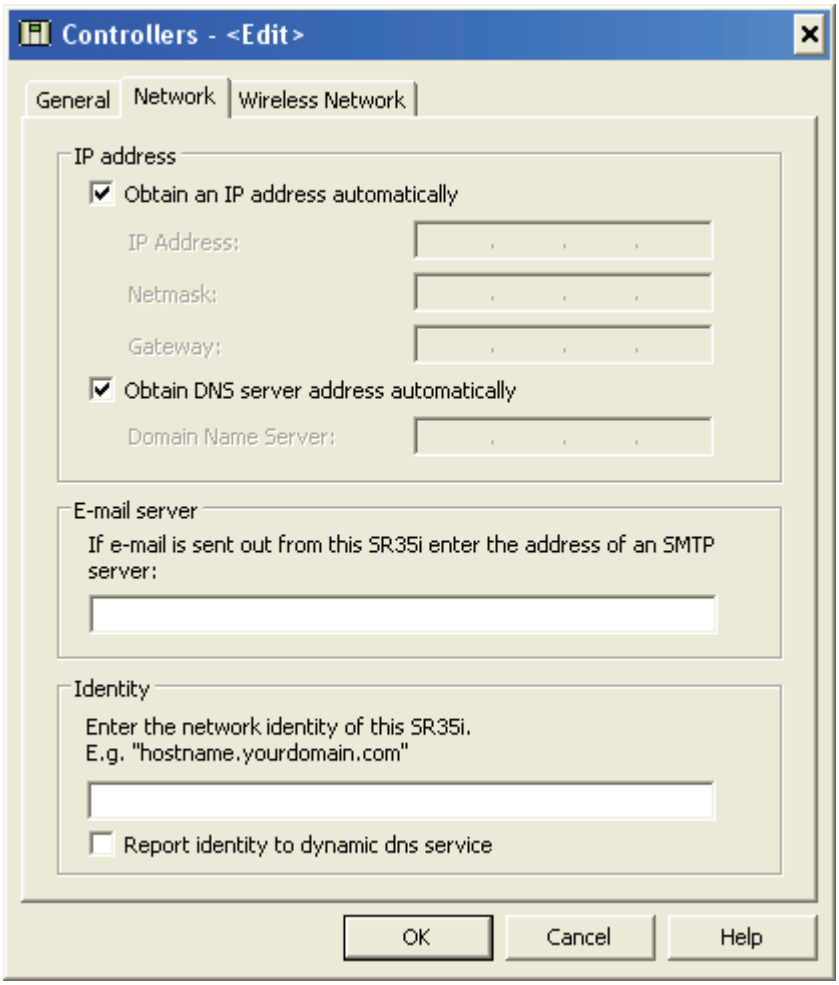
When the system allows for DHCP in SR35i some more settings must be considered.

When DHCP is selected, every controller automatically gets an IP-address and a general DNS (used for later search of IP-address to DynDNS.org).

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Select a SR35i in the tab **Controllers**.
3. Click **Edit** - or double-click the name.
4. Go to the **Network** tab and mark the tick-box **Obtain an IP address automatically**.
5. Enter in the field **Identity** the name for the controller. If DynDNS is used it might be e g House1.dyndns.net, Identity1.dynalias.net or similar.
6. If the controller also is used for **confirmations** in a reservation system, enter the name of the **e-mail server**. This is obtained from the ISP. E g mail1.xyz.com. Be sure the mail server allows for the chosen identities (no blocking).
7. Decide whether the controller must **report its identity** to a DynDNS server.
   - By default it is assumed that this is supported by a router and the “provider” parameter will be set to “inactive” in the SR35i.
     Note that if the SR35i is used as a “subagent” behind a router that reports to DynDNS, the identity of the router must be entered as the identity of the subagent.
   - If you mark the tick-box to report a warning may appear to instruct that a DynDNS account [→ 89] must exist.
8. Click **OK**.
9. Repeat the steps for each SR35i using DHCP.

The screen shot below shows the above settings.



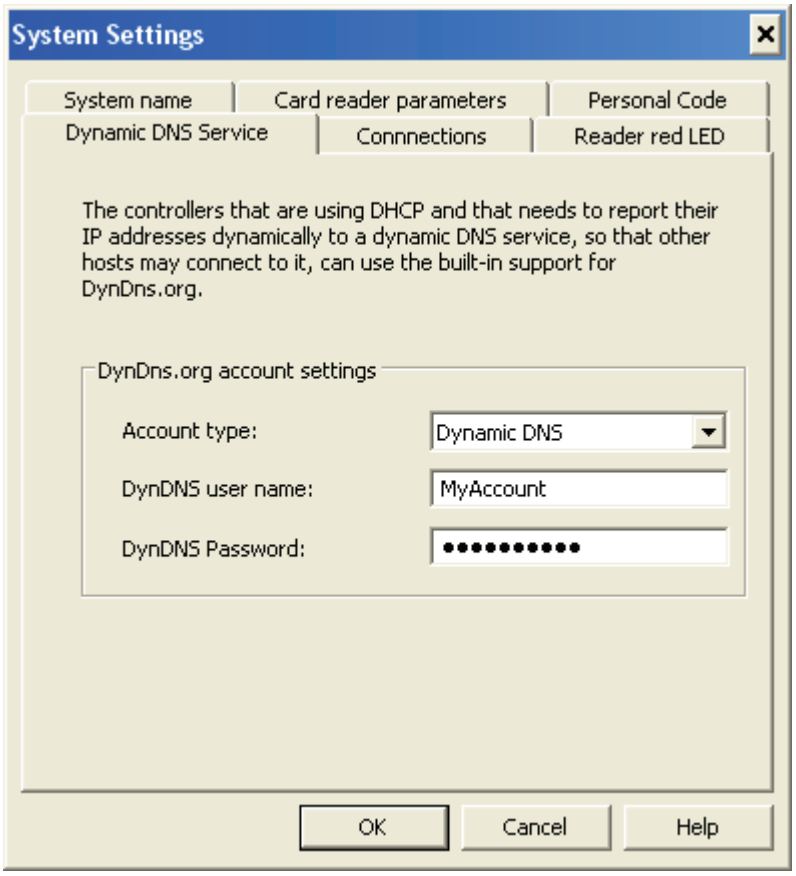
Network setting in the SR35i

21.2 Customize the database for DHCP

If DHCP is used, you must now decide on how the segment controller should communicate with each other. All SR35i using TCP/IP must have the Proxy tick box marked.

Proceed as follow to allow for DHCP-function.

1. Open Installer [→ 76] application.
2. Choose on the menu **System** > **System settings**.
3. Click the **Dynamic DNS Service** tab.



⇨

4. Use DynDNS.org and enter the **Account type**, **User name** and **Password**.
5. Finished

21.3 Prepare the SR35i component for DHCP

If the SR35i will use the DHCP function, this must be configured in each unit.

Dependant of how the network is configured related to the PC in use (routers, firewalls etc) some or all parameters have to be configured locally by means of the keypad and display in the SR35i.

The main setting is to use DHCP.

Proceed as follows:

1. Power up the SR35i.
2. Press buttons **2 > 1 > 2 > 1.**
   ⇨ The controller will convert to the DHCP function and search for the IP settings.
3. There are now also options to configure different parameters like DynDNS reporting options.
4. Repeat for all SR35i that needs DHCP.

22 Configure names and functions for doors

The next step is to configure names and functions for the connected doors. Dependant of the type of door unit different menus is visible. The example below applies for a DC22 door controller.

1. Open the Installer [→ 76] application.
2. Click the **Doors** tab. You will see the installed, addressed doors as **C1:D1, **C1:D2 etc.

If an installed door is missing in the list, it means that the system has no communication with that door.

3. Select the desired door (if it is not already selected) and click **Edit**. Tip – You can also right-click and choose *New*, *Edit* or *Delete*.
4. In the **Name** field, enter the name for the door. Maximum 32 characters.
5. Check that the proper reader type is shown in the **Terminal type** field. If you are using zones, there may be a choice of readers if an EXIT reader is installed.
6. Click the **Relays tab**.
7. Select the checkbox **Use relay for alarm by-pass** if a Monostable alarm (locally) will be used in this door. It can belong to a bistable alarm zone but cannot physically connect to the Intrusion Alarm Control unit.
   Monostable function. Used if you want to by-pass the alarm for a short amount of time (e.g. for an entrance). The by-pass time is equal to the opening time + the door held warning time. Doors with Monostable function cannot connect and control the zones in an intrusion alarm.
8. If the door central shall control a motor lock mark the tick-box for **Motor lock**
9. Click the **Door control** tab.
10. If door monitor contacts are used, click the **Door monitor contact exists** check box. Enter whether the contact is closed or open when the door is closed.
11. If lock monitor contacts are used, click the **lock monitor contact exists** check box. Enter whether the contact is closed or open when the lock is locked.
12. Enter, by choosing one of the alternatives **Lock at once when door is opened** or **Lock when door is closed again**, how the door is relocked after having been opened. This will be dependent on the type of lock installed.
13. If IOR6 lift control is used - see section Lift Control with IOR6 [→ 95]
14. Click **OK**.
15. Continue with the next door until you have named all doors and described their function.

23 Configure IOR6 relay controller

The relay controller can be used for a range of special functions. These are at the moment:

- Door lock monitor - output
- Common alarm (pulse) - output
- Time control - output
- Monitoring a power failure signal (e g battery) - input
- Monitoring an “Emergency“ opening signal to open selective doors - input
- Exit button function. Input for activating a relay
- Reservation functions
- Lift control

Common alarm is not possible in an IOR6 used for lift control applications. You must use another IOR6 in these cases.

The settings for this you find in the Installer – Doors where you mark the actual IOR6 (or create a new). There are separate tabs for relays and inputs.

23.1 Door lock monitor - output

The lock monitor function can be used for monitoring that selected doors are unlocked (e g emergency exits).

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab **Doors** and mark an IOR6.
3. Click **Edit**.
4. Mark the tick box for **lock monitor** in the tab **IOR Relays**.
5. Select the lock monitor function for any of the relays.
6. Click on the button to the right of the list box.
   ⇨ A new window with a **door list** is displayed.
7. Select which doors to be monitored.

23.2 Common alarm – output

The common alarm can be set to two different output types:

- **Pulse mode** means that the relay falls back after a certain time.
- **Bistable mode** means that the system will keep any activated relay state until the user performs acknowledge – or another decided event occurs.

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab **Doors** and mark an IOR6.
3. Click **Edit**.
4. Mark any of the tick boxes for **Common alarm** in the tab **IOR Relays**.
5. Every relay in the IOR6 can optionally be configured for generating an output signal. Select function in the list-box.
   - If **pulse mode** an event filter can control the relay. Set the **time** the relay shall be active.
   - If **bistable mode**- a new menu is opened where the criteria for the relay is further selected.

23.3 Configure IOR6 for time control

It is possible to use any IOR6 relay as a simple timer function (similar to a door opening relay).

These relays will be displayed in the Entro program and allow for choosing individual time schedules for them.

The system allows for separate opening time for the relays as well as relays 1 – 4 which can be activated via input signals (remote opening).

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab **Doors** and mark an IOR6.
3. Click **Edit**.
4. Choose tab **IOR6 Inputs**.
5. Open the Entro application to select further options like Time s schedule and unlocking time.

23.4 Power failure warning - input

Inputs can be setup to monitor signals from power supplies. Often used when a battery-backup power supply is installed. E g a signal can be sent from the PSU when the mains falls and batteries are used. Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab **Doors** and mark an IOR6.
3. Click **Edit**.
4. Click the tab **IOR6 Inputs**.
5. Click the list-box and choose **Power failure**.

23.5 Emergency opening – input

An input can activate a function to set **selected doors unlocked**.

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab **Doors** and mark an IOR6.
3. Click **Edit**.
4. Select **Emergency opening**.
5. Click on the button to the right of the list box.
   ⇨ A new window with a door list is displayed
6. Select doors that should be unlocked when the input is activated.

23.6 Exit button - input

It is possible to set an input to activate a relay at a certain time. E g using a remotely open reservation door or allow for pushing a button in lift.

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab **Doors** and mark an IOR6.
3. Click **Edit**.
4. Click the tab **IOR6 Inputs**.
5. Select **Exit button** (if not selected already).

23.7 Configure IOR6 for Reservation system

If any of the relays in an IOR6 are going to be used in a Reservation system, follow these instructions:

1. Open the Installer [→ 76] application
2. Click the **Door tab**. Normally a new IOR6 is displayed as **Cx:Dy in the list of doors. Mark this, click Edit and step to item 7 below.
   If you manually want to create a new IOR6 – proceed as follows:
3. Click **New**. The **Door properties** are displayed.
4. Enter the name of the relay controller in the **Name** field.
5. Check and/or enter the address.
6. In the list box **Terminal type** - select IOR6.
7. Click the **IOR6 Relays** tab.
8. Mark the tick box Reservation door and/or Reservation machine.
9. Enter the name of each relay with digits. They will later be shown as the name of the IOR6 + the relay number.
   E g if the IOR6 is named “Washing room” and relay 3 it is shown as Washing room:3
10. Click on the list box on each relay and activate them as follows:
    - **Reservation – Door**. Means it will be used as an ordinary door opening relay and is activated for a specified opening time.
    - **Reservation – Machine**. Means that this relay is activated the *whole* time the object is booked (e g a washing machine). Note if any **time shift delay** is to be applied – please read more about setup zones for reservation object [→ 104] .
11. Click **OK**.

23.8 Lift Control with IOR6

When applied to lifts, SiPass Entro can be used to restrict access to the different floors in a building. For lift control up to 32 IOR6 relay controllers can be connected to the SiPass Entro system, which means that altogether 192 floors can be controlled.

Note that neither IOR6 nor its master reader can be included in zones. The lock relay of the master reader (door controller) cannot be used for any applications.

1. Open the Installer [→ 76] application
2. Click the **Door** tab. Normally a new IOR6 is displayed as **Cx:Dy in the list of doors. Mark this, click **Edit** and step to item 7 below.
   If you manually want to create a new IOR6 – proceed as follows:
3. Click **New**. The **Door properties** are displayed.
4. Enter the name of the relay controller in the **Name** field.
5. Check and/or enter the address.
6. In the list box **Terminal type** - select IOR6.

7. Click the **IOR6 Relays** tab.
8. Mark that this IOR6 will be used for lift control.
9. Enter name of each relay with digits. They will later be shown as the name of the IOR6 + the relay number.
   E g if the IOR6 is named “Lift A” and relay “3” it is shown as Lift A:3
10. Click on the list box for each relay and activate them.
11. Click **OK**.
12. Click the tab **Doors** and mark the terminal intended as a **Master** for the IOR6.
13. Click on **Edit** and click the tab **Lift Control** and mark the IOR6 -units that will be controlled by this terminal.
14. Click **OK**.

A suitable name for the master door terminal is e.g. “Lift, floor”. Door terminals are named on the Doors tab

In the Entro application, the numbered floors (relays) are shown on the **Access groups** tab, in the door list under the name of the master reader. This way, it is very easy to select the floors to which the group should have access.

It is also possible to activate the relays according to the time schedule applied for the actual master reader. You find the set up for this in the IOR tab in the Door menu (in the Entro application). You mark the tick-boxes in the time zone column for the relay to be activated. Relay 1 – 4 in every IOR6 can also be activated via a signal to exit button input (remote opening).

24 Configure Intrusion Alarm zones

SiPass Entro offers different methods to **arm** a bistable intrusion alarm zone:

- Using a valid card at the door terminal.
- Using a pushbutton connected to the Alarm button input.
- Using an external timer connected to the Alarm button input.
- Using a SiPass Entro Alarm time schedule (automatic).
- Using the door icons in the Door and Event Monitor program (right-click).
- Use the intrusion alarm maneuver functions. The alarm panel status signal is used to “follow” the status of the intrusion alarm controller (feedback).

To **disarm** the alarm; following methods are valid:

- Using a valid card at the door terminal.
- Using the door icons in the Door Monitor application (right-click).
- Use the intrusion alarm manoeuver functions. (The alarm panel status signal is connected to the ASF input).

NOTE 1

Remember that any zones (e g Alarm zones) will work best if they reside in the same sub-net when several SR35i use TCP/IP (between related SR35i).

NOTE 2

Remember that any DC22s configured for Monostable alarm cannot be wired for controlling any zone in the intrusion alarm.

In cases where only one door is used to control an intrusion alarm, you must still create an alarm by-pass zone for that door. Note that an alarm by-pass zone can be combined with both roll call and entrance limitation - but not with anti-pass back.

1. Open the Installer [→ 76] application.
2. Click the **Zones** tab, then **New**.
   For *new* zones a wizard is invoked which will help you configure the required functions. For existing zones the tabs are shown (displaying the same information).
   Tip – You can also right-click and choose New, Edit or Delete.
3. Type the name of the zone in the **Name** field.
4. Select **Alarm zone**. You will also see any other functions this zone can be used for.
5. Click **Next**. In the **Entry doors/Available** box, select the door/s to be included in the alarm by-pass zone.
6. Click **Next**.
7. Select the door, which is **physically connected** to the intrusion alarm control unit.
8. In the **Alarm by-pass relay operation** list box, select the alarm control method to be used.

- **Bistable function**. Used if you want to fully control the intrusion alarm. You may deactivate the alarm (after it has been activated) by using your card at the reader and entering your PIN. To activate the alarm, press B and use your card at the reader (or B + card + PIN). You can use a push button (if fitted) connected to the alarm activation input of the DC22. Automatic alarm activation can be achieved by using a specific time schedule for alarm control.
- **Bistable pulse** This alarm by-pass method is similar to bistable function, but instead of the output remaining operated, a short pulse is generated for both the switch-on and switch-off operations.

9. Decide if the **Alarm activation warning** shall be used. In case enter, in the warning time field, duration for how long a warning buzzer should sound before the alarm is activated (between 5 - 1000 seconds = 16.5 minutes). The buzzer warns people still in the building that the alarm is about to be activated. During this time the pre-warning alarm relay output will change state in all DC22 included in the actual alarm zone.
   If you decide to **not use** warning the alarm by-pass relay changes its state *immediately* – without any buzzer warning (pre-warning). If the ASF function is enabled the exit button still works until a valid ASF signal occurs. This will be the case if the intrusion alarm takes care of the pre-warning (= not yet any ASF).
10. Select if the **Exit button** is allowed to abort the alarm activation cycle.
11. Choose which **Time Schedule** will be used for time controlled alarm activation. If you do not select any you have to manually activate it – or use an external signal (connected to the input for alarm activation).
    If you have not created time schedules (in the Entro program) – you click on the clock icon and select New, Edit or Duplicate a time schedule.
12. Click **Next**.
13. Mark the tick box **Use Alarm Status Feedback** if the intrusion alarm's status signal will be connected. This signal connects to the ASF in the DC22. It tells SiPass Entro that the Intrusion Alarm has been activated (or deactivated).
14. In the field **Timeout for ASF** you write the time in seconds, SiPass Entro will wait for the status signal – before it is seen as an activation failure. In this case SiPass Entro will go back to normal state (and accept normal accesses).
15. Mark the tick box **LED Control** to define how the red LED at the door terminal will be controlled. Either the LED is controlled by the feedback signal - or another external signal could be connected. This is the case if the red LED needs to flash in some way.
    - If choosing ASF – you optionally also can disable the red LED after a certain time (after alarm activation). In this case the LED will light **only** on the reader where the command is performed. Any other reader LED in the zone will be off.
    - If you do not choose the ASF function – an external signal could still be connected. In this case choose only LED Input.
16. If you click on **Adjust** (at LED input) you can adjust the time to determine if the external signal from the alarm system should light or flash the red LED on the door terminal. Default (and maximum) value is 3.2 seconds. If it should flash – this period should be slightly longer than the pulse cycle of the external signal.
17. Click **OK**.

24.1 Decide on security levels for alarm control

1. Open the Entro [→ 76] application.
2. Click on **Zone** tab.
3. Click on **Settings**.
4. Select the **security level** for activating and deactivating the intrusion alarm.
5. Click on the list box and choose Card or Card+PIN.
6. Click OK.

This selection will be set for all Alarm zones you create.

25 Configure other type of zones

In the same way as an alarm zone is created one or more doors can form another type of zone. These could be:

- Anti pass back zone
- Roll call zones
- Entrance limitation zones.
- Interlock zone (two doors)

You can also use sub-addressing technique when creating zones and selecting readers. This applies to reader type BCLINK, who can be addressed as ENTRY or EXIT when connected to the same door central.

25.1 Anti-pass back/Roll call

As an anti-pass back zone is created a roll call zone is created as well. You can however create zones that are roll call zones only.

The only difference between roll call and anti-pass back is that anti-pass back means that the card will be black-listed if a person does not use his card to leave a zone he has previously entered.

The same reader can be an IN reader to one zone and an OUT reader to another.

This is how to create an anti-pass back or roll call zone:

1. Open the Installer [→ 76] application.
2. Click the **Zones** tab, then **New**.
   For new zones a wizard is invoked which will help you configure the required functions. For existing zones the tabs are shown (displaying the same information).
   Tip – You can also right-click and choose New, Edit or Delete.
3. Type the name of the zone in the **Name** field.
4. In the **Entry doors/Available** box, select which is reader IN.
5. In the **Exit doors/Available** box, select which is reader OUT.

If a person violates anti-pass back, i.e. does not use his card to leave a zone and then tries to enter the same zone or another zone, the card will be blacklisted. This function is used to specify for how long the card should be blacklisted.

1. Open the Entro [→ 76] application.
2. Choose the **Zone** tab.
3. Click on the button **Settings**.
4. Click the **Anti-pass back** tab.
5. Choose the desired alternative.

25.2 Entrance limitation

When you create this type of zone you then have to decide which access groups will be able to enter the zone. You will also need to specify the counter for each person.

1. Open the Installer [→ 76] application.
2. Click the **Zones** tab, then **New**.
   For new zones a wizard is invoked which will help you configure the required functions. For existing zones the tabs are shown (displaying the same information).
   Tip – You can also right-click and choose New, Edit or Delete.
3. Type the name of the zone in the **Name** field.
4. In the **Entry doors/Available** box, select the doors to be included in the zone.
5. Click **OK**.
6. Open the Entro [→ 76] application.
7. Click the **Zones** tab.
8. Mark the name of the entrance limitation zone and click on **Edit**.
9. Click on **Entrance limitation** and select restriction type (both types can be selected).
   - **Decrement entries counter**. Means that a certain number of entries are granted in doors included in this zone. Later, in the Entro application, one or more access groups should be created with restricted access to these doors. Finally, the number of granted entries can be specified for each person.
   - **Limited access to this zone** (e.g. twice a day). If this alternative is selected, go to the Settings of limited access box and select the desired time restriction, e.g. twice a day. If needed, access can be limited further by choosing restrictions per time interval.

If more than one entrance limitation zone is created, only one zone can have limited access

25.3 Interlock zone

SiPass Entro offers the possibility for two doors to co-operate in order to form an interlock zone. This means that the first door has to be closed before the next door can be unlocked.

To be able to monitor the status of the doors, both must be equipped with **door monitor contacts**.

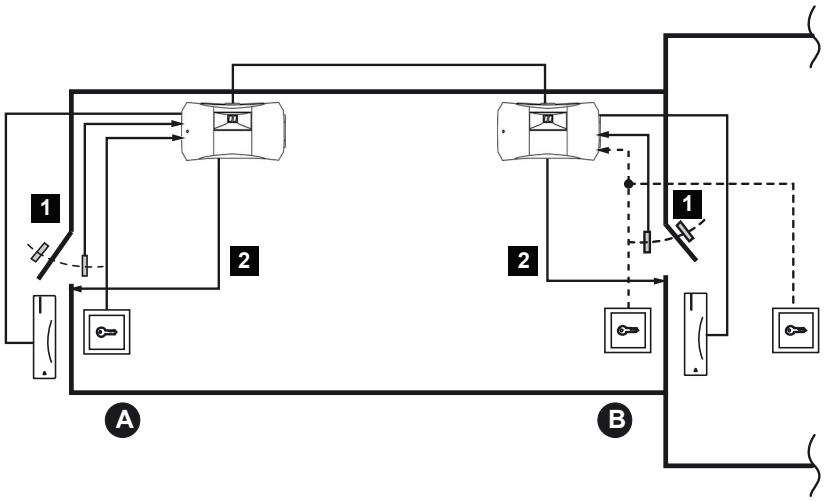
Proceed as follows:

1. Open the Installer [→ 76] application.
2. Choose tab Zones and click on new.
   ⇨ A wizard starts
3. Enter a **name** and select **Interlock**.
4. Select the **two doors**.
5. Select if the **second door** in the zone should open automatically – or not.
6. Exit.

If security level is "**toggle card**" on a door in an interlock zone the "second" door does NOT open automatically when the first door is closed.

25.3.1 Example Interlock

The **Door (A)** has a card reader to the zone and an exit button from the zone. The **Door (B)** may have exit buttons in both directions – or have a card reader to the zone. Depending on the type of installation, the interlock zone operates slightly differently.



Example with two BCLINK readers PR500

1.	Door monitor contacts.
2.	Electric Lock.

Access from Door A to Door B

After entering door A, which is then closed **during** the opening time, door B will be automatically unlocked.

However - if door A is closed **after** the opening time (e g while the buzzer sounds during the Door Held Warning Time), the exit button must be used to enter door B. If no button exists at door B - access must again be made from outside door A.

Access from Door B to Door A

After entering door B, which is then closed during the opening time, door A will be automatically unlocked. If door B is closed after the opening time (e g while the buzzer sounds during the Door Held Warning Time), the exit button must be used to enter door A.

If only exit buttons are installed in door B, no automatic unlocking will take place. The Exit buttons have to be used for both doors.

26 Configure for reservation

26.1 Setup zones for reservation object

This section describes the steps for creating the doors and relays in a Reservation object. Note that a common main reader for more than one reservation object will only work if the objects are grouped together.

1. Open the Installer [→ 76] application.
2. Click the **Zone** tab then click **New**.
   For new zones a wizard is invoked which will help you configure the required functions. For existing zones the tabs are shown (displaying the same information).
3. Enter the name of the object in the field **Name**.
4. Select **Reservation object** and click **Next**.
5. Click on **Add/Remove doors** and a new window is displayed with all SiPass Entro doors and all IOR6 relays specified for reservation use.
6. Add units to the Reservation object and **Click OK.**
   ⇨ A list of doors/relays are displayed and completed with a new option field.
7. For **each door (or relay)** you now have to configure the function of them by choosing one of the following:
   - **Main reader.** This is indeed the object you may reserve. E g 18:00 – 19:00. Note that this option will only be valid for one door (reader) – all other doors in the object will then be blocked for this selection.
   - **Reservation time**. This may be a door “on the way” to the object and no time shift is added.
   - **Time shift**. This door (or IOR6 relay) will allow for access only during a time shift (specified below). E g time shift set to 30 min will result in access 18:30 – 19:30. Remember that doors/relays of this type can **only belong to one object**.
   - **Combined time**. This is a door that will allow for access the time for the Main door plus the time shift. E g 18:00 – 19:30
8. Enter the **time shift delay** (maximum 120 minutes) if any door is using time shifts.
9. Click **OK**.

Repeat for any other new reservation objects to configure.

If any relay controller IOR6 are used in the reservation object you configure these according to the section Configure IOR6 for Reservation system [→ 95] .

Supplementary parameters for reservation are configured in the Zone tab of the Entro program.

26.2 Random allocation or NOT of similar reservation objects

If several similar objects are to be available for reservation, you can randomly allocate them to minimize the wear on individual equipment.

If choosing to use random, mark the tick box **Random** and read more in the section Reservation object (group).

An example of random function might be a laundry room with a couple of washing machines, where each is an object, which will be controlled by a relay in an IOR6 (machine control). All these individual objects are then grouped together and can be treated as one common, **grouped object**. The users are then allotted some of these individual objects when a reservation is done.

To create a grouped zone:

1. Create the individual objects as above.
2. Select the same **Main Reader** for all objects.
3. Select an IOR6 relay (as machine control) to control the object (e g a washing machine).
4. Finally you create a new object but select **Group of Reservation Objects** instead and mark the actual objects to group. Note that a common main reader for more than one reservation object will only work if the objects are grouped together.

Doing this, will result in the main parameters (e g the maximum number of reservations) being the same for all objects.

26.3 Alarm control in a reservation object

If you install an intrusion alarm in premises that are also using reservation, you can use the card reader for alarm control in both Monostable and bistable mode. You use a DC22 for this.

Monostable mode

This method requires that the DC22 used in the door must be configured for Monostable mode. In the tab Relays (in the door properties of the Installer program), mark the tick-box **Use the relay for alarm by-pass**.

The alarm by-pass relay will change state during the **Opening time** + the **Door Held Warning Time** - and will the automatically fall back.

Bistable mode

Note that this method differs somewhat from the way SiPass Entro normally treats intrusion alarm control (within alarm zones).

This mode will arm or disarm an alarm section in the intrusion alarm. Connection is done to the alarm by-pass relay in the **DC22**. Be sure that the tick-box **Use the relay for alarm by-pass** in the Relays tab is **not** marked.

The actual zone in the intrusion alarm can only be managed from this door.

- **Activation** is performed with an alarm button connected to the Alarm button input of the DC22.
- **Deactivation** is accomplished by a granted access to the reservation object. Usually the security level Card or Card+PIN will apply.

26.4 Time schedules

The first thing to do is to identify the times for reserving. In tennis court there may be three-hour sessions, which can be booked all the week around – or some other object only available on weekdays.

In the system there can be 32 time schedules with each 24 intervals for reservation.

The clock and day values below forms the basic intervals but it can be modified in some aspects by the “time shift” concept. You add this function in the Installer program when configuring the doors in the reservation object (zone).

1. Open the Entro [→ 76] application.
2. Click the **Time schedules** tab.
3. Click **New**.
4. For new time schedules a wizard is invoked which will help you configure the required functions. For existing time schedules the tabs are shown (displaying the same information).
   The wizard also directly allows for configuring of Half days, Holidays and Holiday periods. See Enter public holidays and holiday periods.
5. In the **Name** field, enter the name of the time schedule e.g. Training sessions.
6. Click **New** to create a new **Interval**. A row with suggested fields with From, To and Weekdays is displayed.
7. Click on the arrow at **From** and choose time. Press TAB.
8. Click on the arrow at **To** and choose time. Press TAB.
9. Select the **Days** when the interval should be valid.
10. Repeat step 4-7 for every new interval.
11. You can click on **Sort** to get the intervals sorted.
12. Click **OK** to save the time schedules.

Set up information for the next time schedule in the same way.

26.5 Reservation object

Below describes how to configure the Reservation object itself.

The definition of physical doors/relays for the single or grouped object is initially done in the Installer [→ 76] application.

1. If more than one Member class shall be used – go to the folder Person settings in the **System > System settings** menu and decide on the general names for **classes** one, two and three. This will then be visible in each object for further defining of values.
2. Open the Entro [→ 76] application.
3. Click the tab **Zones**.

   ⇨ The previously defined objects are displayed.
4. Mark the object and click **Edit**.
5. Select the **Time schedules** from the list. Click on the arrow to list available time schedules.
   You can also click on the clock icon to Create, Edit or Copy a reservation time schedule. Then choose the desired time schedule by clicking the name.
6. Mark if flexible reservation within an interval should be possible. Read more in the Flexible reservation in same interval section.
7. Enter how many **Maximum no of concurrent reservations** on the same object will be allowed. E g if a tennis park has two separate courts but only one door, two different member groups must still be able to book the same time. Max value is 99.
8. Click the tab **Max nr limits.**
9. Decide on the users **reservation capabilities** for a certain advance period. E g to book four training sessions in a month in the same object. Max value is 60 on each.
10. Choose if even more restrictions should apply for each class. Enter in the field **Max nr** and **Calendar period** the number of reservations (maximum 6) a member group can make in a certain period (day, week or month).
11. Click the **Time related restrictions** tab.
12. Enter in the field **Max forward reservation time** for how long a period booking is available. E g 31 days. Max value is 365 days.
13. Decide on how many minutes the system waits until an automatic cancel is done. Enter in the field **Automatic cancel time**. This gives a delay before some other Member group can book the same time. Max value is 60 minutes.
14. Enter the allowed **Overlap time** for accessing the object after the reserved time. This makes it possible to enter a booked tennis court some minutes later (due to a traffic jam or similar). Max value is 99 minutes.
15. Enter how long, in hours and minutes must **remain of an interval** to allow for a new reservation. Maximum value is 23 hours, 45 minutes.
16. Click **OK**.

Repeat necessary steps for each reservation object.

26.6 Enter public holidays and holiday periods in Reservation

Certain day's reservations might not be available. E g if tennis court is used for a tournament – or if a golf court has closed for the season.

See also section Service mode [→ 110] for another type of exception.

In the ordinary SiPass Entro system there are *Public Holidays and Holiday periods,* which allow exceptions from an ordinary week. These can also be used in the reservation system to inhibit reservation at these times.

In most cases they will not coincide and must be specified for each separate time schedule – in the Reservation.

To make the system understand that holidays and holiday periods should not be treated as ordinary working days, this information must be configured.

Proceed as follows:

1. Open the Entro [→ 76] application.
2. Click **Time Schedules** tab.
3. Select the time schedule; click **Edit** and then the **Public Holidays** tab.
4. Mark the tick in the **Use Global Public holidays** – if you prefer to use the same dates as specified in the main Entro program.
5. Click **New**. The **Public holidays** window is displayed.
6. In the **Date** field, enter the date of the first holiday, or click the **Calendar** button and choose the date. You can have up to 14 days in each time schedule.
7. Click **OK**. The **Public holidays** tab is redisplayed with the date filled in.
8. Click **New** and configure the next holiday accordingly. .
9. Create the **Holidays** in the same way – but enter both **Start** and **End** date. You can have up to 4 periods in each time schedule.
10. Repeat steps 4-8 for every separate time schedule in the reservation system.

26.7 Decide on reservation authorities for access groups

1. Open the Entro [→ 76] application.
2. Click on the tab **Access groups**.
3. Create or select an access group
4. Go to the tab **Reservation** objects.
   - If you also select the tick box Caretaker this group will be able to access (and use) this object 24 hours a day – without any reservation. (Normally you create a separate access group with this functionality).
5. Select one or more of the available **objects** to be accessible for this group.
6. Click **OK**.

26.8 Give persons reservation authorities

In a reservation system it is important that every person has a Member group no even if it is the same for all persons. Otherwise the person cannot reserve any times.

Note! We only describe additional information regarding Reservation.

Every person must belong to one or more access groups simultaneously. These may already been given reservation rights.

If not - you first create a new access group and proceed as follows:

1. Open the Entro [→ 76] application.
   ⇨ The **Persons** tab is displayed.
2. Mark a person and click on **Edit**.
3. If you enter a persons' e-mail address in the **Free field**, SiPass Entro can confirm a reservation by sending an e-mail message (if the software is configured for this). See paragraph Prerequisites for confirmations [→ 112] .
4. Check or choose correct **access group**.
5. Now decide on the Member group settings. All persons belonging to the same member group will automatically have the same rights in the reservation system. These may be e g training groups, families etc.
   There exists two methods of entering the parameters depending of the numbers of Member classes previously configured in the object:
   - **Default one class** – Enter only the **member group nr** direct on the general tab (above the card number).
   - **Two** or **three classes** – also click on the **Member group settings tab** and select a **Member class**. You will see all persons in the same member group
6. Click **OK**.
7. Repeat necessary steps for every person.

NOTE 1

Check that the access group allocated to a person has the correct reservation object associated (see Access groups).

NOTE 2

You can simplify the configuring of cards/persons even for the reservation by using the Duplicate function.

26.9 Flexible reservation in same interval

In many cases, such as conference rooms, you do not want to be restricted to reserving one or more short intervals – you would rather have a more flexible way to reserve times.

The software allows for defining a longer interval (e g 8 AM to 6 PM) where the user then can reserve a flexible time within this interval. I e you first restrict the total outer limits (start and stop) but the user can reserve the whole or part of it.

Proceed as follows:

1. Open the Entro [→ 76] application.
2. Click the tab **Zones**
3. Mark the actual reservation object and click on **Edit**.
4. Create or Edit the time schedule to be used. Normally this results in fewer - but longer intervals.
5. Mark the tick box **Accept flexible reservation periods** on this object.
6. Click **OK**.

26.10 Show reservation information to the user

If some kind of maintenance or service is scheduled, it is possible for personnel to set this up in the software. Proceed as follows:

1. Open the Entro [→ 76] application.
2. Click the tab **Zones.**
3. Click on **Settings** and the click the **Web Settings** tab.
4. Select appropriate alternatives – Show Name of Person, Show Member Group Numbers and Show all reservations.
5. Click **OK**.

26.11 Service mode

If some kind of maintenance or service is scheduled, it is possible for personnel to set this up in the software. Proceed as follows:

1. Open the Entro [→ 76] application.
2. Click the tab **Zones.**
3. Mark the object and click **Edit.**
4. Click on **Set Service mode** and select date (by picking in the calendar) and time for start and stop in the list boxes – or mark the tick-box **Until further notice**.
5. Click **OK** and you will see the chosen time. To edit the time just click the same icon again.
   - If you want to delete the chosen time just click **Clear service mode**.
6. Click **OK.**

26.12 Setup for debit function

SiPass Entro has a function for exporting additional information about how reservation objects are used/not used. Any event associated with reservation will have a value .

Proceed as follows:

1. Open the Entro [→ 76] application.
2. Click the tab **Zones** and **Edit** the object.
3. Go to the **Debit** tab. You will see an edit box for each event type.
4. Select a **value** in the form xxxx.yy for each event. The format of the values will follow the Windows format for numbers.
5. Click **OK**.

The system stores these values along with event in the ordinary event files – but does not display them in the event log on the screen.

To evaluate them – use the **Door and event monitor** application and export the result into a text file for further actions in external software.

(Alternatively transfer the information via a BAPSI application).

Note that if you change the debit values according above after the time of the event the original will be exported (= no corrections).

26.13 Configure for e-mail confirmations

SiPass Entro can automatically generate an e-mail message to the person making a reservation (or a cancellation). The texts in these messages are stored in two files in the CF8 (compact flash) memory card and may be edited but this is normally not necessary.

The messages also include the IP-address to the web server (SR35i) that sent the message. This gives an easy way to log in again (for editing reservations).

The name of the SR35i, sending a confirmation, allows only characters accepted in e-mail addresses. Special, national characters cannot normally be handled by the e-mail server (ISP).

26.13.1 Prerequisites for confirmations

The Reservation system uses Internet connections that allow for making reservations on any PC. The prerequisite for this is that the SR35i controller has an available **Internet connection**.

In addition to this you can configure some parameters, which allow for sending a confirmation by e-mail to the person doing the reservation.

The following parameters are defined in consultation with the IT-manager.

Proceed as follows:

1. Open the Installer [→ 76] application.
2. Click the **Controllers** tab.
3. Mark the controllers, which contains the CF8 and will send the e-mail message – and click on **Edit**.
4. Click the **Network** tab and check/enter the IP-address to the **Domain Name Server (DNS)**. This is in fact a server converting the domain name (e g xyz.com) into a valid IP-address. The DNS often resides with the contracted Internet Service Provider (ISP) – or in the local area network.
5. Enter the **SMTP Server** which is the e-mail server handling the outgoing mails. This often resides with the contracted Internet Service Provider (ISP). The name may look like smtpserver.swip.net - or similar.
6. Enter the **Identity** that SR35i uses to create a valid sender address. May be e g xyz.com and is often used by the ISP to further validate the sender.
7. Click **OK**.
8. Finally check that each person has a **valid e-mail address** entered in the free field of the person's properties (in the Entro application).
9. If you have named the SR35i "Reservation" and enter "xyz.com" as domain name – the message is sent from the sender address reservation@xyz.com to the e-mail address entered in the first free field on each person's properties.

26.13.2 Editing text in the confirmations

The actual texts sent are stored in files CF8 memory card and are named:

- reservation.txt (Message sent when reserving)
- cancelreservation.txt (Message sent when canceling)

To change these you make use of a **suitable PC-adapter** for retrieving and storing the contents of the CF8 memory card. As follows:

1. Place the CF8 in the adapter. (Be careful when connecting the card to avoid destroying the data). Use the Windows Explorer or similar to find the files.
2. In the folder “LANG” there are a number of language folders (0, 1, 2 etc.). Locate the file to change.
3. **Edit the file** and write the text you want to display to the user. You then include some optional field tags [→ 114] that (at run-time) will get information from the system (like object, date, time etc.)
   - If you include e g the tag %pfnm the first name of the person will be displayed. See further in section.
4. Store the edited files and **place the CF8 in the SR35i** Controller.

26.13.3 Example of confirmation

Write e g the following text in the file **reservation.txt** and store the file in the CF8.

```
%sbj<Reservation confirmation>
Hello %pfnm,
This is an automatic e-mail message that confirms your
reservation of
%robn, %rhur:%rmin – %ehur:%emin on %rdat/%rmon.
To change any reservation, log on to %ipme/login.html
```

If the person’s first name is Thomas and they have reserved the Tennis court 1 on the 14th of July at 2 – 4 PM, the e-mail message will look like this:

```
Subject: Reservation confirmation.
Hello Thomas,
This is an automatic e-mail message that confirms your
reservation of
Tennis court 1, 14:00 – 16:00 on 14/06.
To change any reservation, log on to
http:xxx.xxx.xxx.xxx/login.html.
```

In a similar way the file **cancelreservation.txt** can be changed. The table in the next section gives more types of information you can include.

26.13.3.1 Table of e-mail fields in reservation confirmations

The table below shows different types of fields, which can be included in e-mail messages. It is the text in the left column that may be included.

Field	Function
%pfnm	Persons first name
%plnm	Persons last name
%pfrf	Persons free field 1 (normally email-address)
%pmno	Persons family/member group
%dnam	Door name
%rwkd	Weekday of reservation - Start
%ryer	Year of reservation - Start
%rmon	Month of reservation - Start
%rdat	Date of reservation - Start
%rhur	Hour of reservation - Start
%rmin	Minute of reservation - Start
%robn	Reservation object name
%ewkd	Weekday of reservation - End
%eyer	Year of reservation - End
%emon	Month of reservation -End
%edat	Date of reservation - End
%ehur	Hour of reservation - End
%emin	Minute of reservation - End
%ipme	IP-address to web server (me) Note! This parameter does not work in DHCP environments. Please write the web address in plain text.

26.13.3.2 Special e-mail fields

The following fields can also be included if other people need a copy of the e-mailed confirmation.

%sbj<x>	Mail subject, x= Subject text
%bcc<y>	BCC recipient, y= e-mail address for secret copy
%rcc<z>	CC recipient, z= e-mail address for copy

27 Maintenance

27.1 Expanding and modifying the system

Expansion and modification of a SiPass Entro system can of course be performed in many ways. Sometimes more doors are needed (sometimes also requiring more SR35i controllers) – or more PCs are needed. In addition software updates and upgrades may apply.

Any expansion needs at least one operating PC connection to handle the necessary setup. There is an option to **reset to the factory crypto key** before any expansion is done.

27.2 RS485

In a system only using RS485 communication (RS232 for PC), just install new segment controllers and door controllers together with new cabling and power supplies. All units will start to communicate immediately.

27.3 Networking

In a TCP/IP based system the segment controllers and PCs must be installed correctly with **correct IP-addresses** and **crypto key**. Door controllers and readers are installed as before.

Controllers are recommended to be of type **SR35i**. It is possible to use the SR34i but the older SR32i (or SR32) cannot be used.

If new SR35i controllers or PCs are to be connected to a TCP/IP based SiPass Entro system, they must be configured correctly. There are two communication “channels” used for information exchange:

- Between PC and SR35i – through RS232, modem or TCP/IP.
- Between SR35i and SR35i – through RS485 or TCP/IP.

If the communication is done via TCP/IP the **crypto key** must be loaded into all units. Initially the default crypto key can be used.

However, if RS232 is used instead for PC-communication, the controller can always be reached.

27.4 Software update in existing system

The version 6.5 supports a migration path from version 4.5 (and later). The new version may include updates for the following components:

- PC equipment
- SR35i
- SR34i (no radio – but adoption to version 6.5 level).
- Door controllers

Before you begin

- Verify which version of the existing PC software (not earlier than 4.5)
- Verify that all Segment controllers are of type SR35i or SR34i.

If any SR32i exist – these must be changed to SR35i. This may also result in that some functionality (e g common alarm) must be “moved” to an IOR6 controller instead.

The following table matrix gives the relevant possibilities for software versions and Segment controllers:

	Ver 4.5	**Ver 4.7**	**Ver 5.x**	**Ver 6.0**	**Ver 6.5**
SR35i	No	Yes *1)+2)	Yes *1)	**Yes**	**Yes**
SR34i	No	Yes *2)	**Yes**	Yes *1)	Yes *1)
SR32i	**Yes**	**Yes**	No	No	No
1) No wireless (RF30) functions. 2) No common alarm relay in the segment controller					

To upgrade to the latest software version, do like this:

1. If the existing PC version is 4.7 or older, first replace all SR32i with SR35i. Then check that all segment controllers’ firmware platform is version 5. Simplest by using the menu system in the controller.
   - If the switching menu does NOT appear in the controller, this means that the controller has been updated to a firmware that instead **supports updates from the PC**.
2. Insert the CD in the drive.
   ⇨ The wizard for updating software is visible.
3. Follow the instructions on the screen. Choose Repair.
4. Open the Installer [→ 76] application.
   ⇨ The installation checks the existing software version and will warn about any possible necessary hardware change (as above). It may give the option to update some units directly (where some may be mandatory for the overall upgrade). This step is similar to SR35i Firmware control [→ 120] .
5. Perform the suggested steps in sequence.
6. Check that the indicators ONLINE and DB UP TO DATE in the lower right corner of the SiPass Entro windows display is green.

⇨ The SiPass Entro system is now updated to a new version and is ready to perform new tasks!

27.5 Installing an additional – or replacing a PC

SiPass Entro version 5.3 onwards allows that several PCs concurrently can administrate the system:

- If only one PC is used the tab “Connection” is not displayed in the Installer application.
- If several PCs will be on-line concurrently the tab “Connections” displays the different names.

Before you begin

Regardless of which above, the new PC must fulfill certain requirements:

- A separate SiPass Entro **software license** must be available for this PC.
- The SiPass Entro program should be installed on a PC with its own, valid **network settings** for LAN connection.
- The PC must have a **valid crypto key** installed – if used. If this has been changed from the default factory – it must be documented and available.
- It is recommended that a **new** PC does not have any old SiPass Entro software or databases installed etc.

If the PC where SiPass Entro runs is about to be replaced (e.g. upgrade to Vista) it may be necessary to upgrade the SiPass Entro software as well. In these cases (where both PC and SiPass Entro is replaced/upgraded), the SiPass Entro system should be upgraded first and **done from the old PC**. After that PC-replacement should take place.

27.5.1 Prepare the database in the existing PC

Proceed as follows:

1. Open the Installer [→ 76] application on the existing, operating PC.
2. Go to the **Connection** tab in **System > System settings** and select that several computers can be connected concurrently.
3. Click OK.
   ⇨ A new tab appears in the main window in the Installer. The default, earlier hidden connection is now displayed as #1. Change the name of it before going further by marking the name, click **Edit** and enter a suitable name.
4. Click the tab **Connections** and start the wizard by clicking **New**.
5. Select **System administration** and enter the parameters:
   - **Name** of the connection (any name)
   - Which **SR35i** – we recommend using the same SR35i for all PCs unless a serial port (RS232) is to be used in the new PC.

- **License number** – I e the number for the new computer. This is noted on the CD case for the new software license.
- **Type of communication** – TCP/IP, RS232 (or modem).

⇨ You have now created a new connection for SiPass Entro and can exit the program in the existing PC.

27.5.2 Configure the additional – or replaced PC

Because this PC does not yet have any database stored nor know the way of communicating with SiPass Entro, you have to create a *connection* also in this PC.

1. Start the **new PC** and install the SiPass Entro software. **Note! A separate software license is needed for a second PC**.
2. Open the Installer application and select at login that a **new connection** shall be created (for a new PC) or an **existing connection** used (for additional PC). Follow the instructions on the screen (similar to above).

   ⇨ You have now defined in which way the computer will communicate, entered the system name, login details etc.
3. Note – if the Crypto key has been changed before the login will fail. Instead perform also these steps:
   - Open the Entro application (OFF-LINE).
   - Enter the 32 character Crypto key manually (in the System menu).
   - Shut down SiPass Entro completely by right-clicking over the icons and select **Exit** (the crypto key will be stored in the database in *this* PC).
   - Start the Installer again – and the actual crypto key will work and the connection should be established.
4. Wait for an updated database (icons are green).

27.6 Installing an additional – or replacing a SR35i

The reason for this is adding an additional controller, replacing a working one (more capacity) or replace a broken.

There are several ways to configure a SR35i before connecting it to a system. Sometimes it is easiest to use the RS232 port.

Remember that the SR35i have built-in menu commands for checking and editing different parameters.

Before you begin

- Consider the risk of electro static discharge (ESD) and take actions to avoid this.
- Ensure that the **controller is erased** (e g via removing the battery).
- Be sure the **battery is not empty**. Especially if the controller has to be shut down and moved after programming.
- That all details about the system parameters are known. Also the *system name* should be known (in case of a PC setup)

It is important that the set-up is correct. This means:

- Correct **node address** (set with knobs).
- Correct **networking parameters** (IP address, Netmask and Gateway).
- Correct **crypto key**.

In some network solutions you will get help from the software to “find” a new SR35i (node) if the default crypto is used. The condition for this is that it exists within the same “subnet” as the PC (which sends a request when starting the Installer program). If a SR35i is found you can add it and configure it like the other controllers.

If the conditions for the above are not met - proceed as follows:

1. Select an **address** for the new SR35i – and power it up.
2. Set up the **networking parameters** (e g IP address) **using the keypad** and display. (Eventually you must erase the memory of the SR35i.)
3. If the **Crypto key** has been changed before in the system, it should be **temporary set back to default** (= same as the SR35i factory setting). Otherwise the controller will not communicate. Go to Entro program and **Change Crypto key** in **System** menu.
4. Connect the network cable and start Installer.
   ⇨ The new controller will be found by the software and is shown as **Cxx. The database and the crypto key are sent or verified from the PC - to the controller. Note that firewalls etc may require that some SR35i have to be setup manually (no **Cxx displayed).
5. Change **name** and set-up the **parameters** for this controller.
6. Wait for an updated database (icons are green).
7. Do not forget to change the **Crypto key** and note it down.

27.7 Installing more readers

It is very easy to install more readers in the system. You only need the necessary cabling and ensure the following:

- A free DC12 or DC22 are available for the reader. (Does not apply for the PD30-EM/PD40-EM).
- That the hosting SR35i does have enough addressing capacity.
- That the power supply has enough capacity.
- That the RS485 bus termination resistors are installed properly.

27.8 SR35i firmware control

Sometimes when a system is expanded or upgraded there maybe need for patching the firmware in the segment controllers. As soon as the Installer program is on-line with the system it checks and inform the user about any updating needed.

In the Installer program there are functions for controlling the mechanism of patching the segment controllers. The status of the different units is displayed.

You can also see the estimated time. This applies for all controllers – not only the one connected to the PC.

The download is using the current files stored in the Entro program folder. File type “SR_firmware.hex” stored in the Entro program folder. It is possible to download an old version.

Proceed like this for the actions you want to do:

1. Open Installer [→ 76] application.
2. Choose **System > System information**.
   ⇨ All controllers are listed on the screen showing the status for the different units (address, product, version, voltage level). If any controller fails to communicate there is a cross over the unit.
3. Click on **Update firmware** – and select which version to download.
4. Click on **Next** and mark the controller to be updated. **We strongly recommend that only one controller at a time is updated!**
5. Click on **Finish**.
   ⇨ A progress bar is displayed for each controller showing the remaining time.
6. You can cancel the process at any time by clicking **Cancel update**.
   ⇨ No update is performed and the old version remains.

27.9 Saving/restoring database on CF8

Normally the SiPass Entro database is stored in all PCs and all Segment controllers.

The installer may also use the menu system in the SR35i (SR34i) to store or re-store the database to/from an existing CF8 memory flash card. However – this method shall be considered as an emergency operation and **must be used with caution**.

You should be very skilled and experienced with SiPass Entro before using this method. In doubt – please contact Technical support.

27.10 Door controller firmware control

If the door controllers DC12/DC22 and the PD40-EM/PD40-EM have firmware **version 1.20** or later, the Installer program can download new firmware via the system bus. This requires that the units are on-line.

During download the door is unlocked if this is defined in the Security level in off-line condition. All other selections results in a locked door.

27.11 Printout of system configuration

In the Installer program you can generate a graphic view of installed components for easier control of e g current firmware versions etc. Proceed like this:

1. Open Installer [→ 76] application.
2. Choose **System >System information**.
3. Click on **Save as** – as an image in JPG format is stored on disk.

27.12 Migrating from a Entro Lite system

When migrating from a SiPass Entro Lite system there are some considerations must be taken:

- The database used in SiPass Entro Lite allow for **card holder names** up to 50 character. When an import is done to SiPass Entro only the 32 first is imported.
- If the **Duress** function is used (in the DC800 controller) this must be “moved” to an IOR6 relay [→ 93] controller and the SiPass Entro configured for that. This applies even if the DC800 still is used as a door controller in the new system.
- Also if the Alarm bypass function is used, considerations must be taken to redesign the solution.

27.13 Uninstalling Entro

To uninstall the SiPass Entro, use the Windows system. There is no special menu choice for uninstalling.

After uninstall the following files are kept for future references. If a complete removal is desired, proceed as follows:

1. Go to the Windows users profile folder. Example for Win XP: C:\documents and settings\Username\.
2. Remove all SiPass Entro files under “Application data” (dbpath.ini, entro.ini database- and event files).
3. Go to C:\Program files\Common files.
4. Delete the complete folder “Bewator USB”

28 FAQ

28.1 Advanced information about LAN

The following chapter contains questions and answers regarding SiPass Entro when used in local area networks and is primarily aimed at IT-managers.

What does the traffic load look like when it is using Entro in TCP/IP LAN?

As SiPass Entro/TCP is evolved with RS485, the traffic is relatively moderate providing that the database is hard packed. The traffic SR35i will have a socket open to every other SR35i. This socket is alive and is tested for failures with a special ping-message every eight second. This is not an ICMP-ping, rather a common TCP/IP package with some information (only a few bytes in size).

Beside this, in an idling system, there is a comparing-of-databases message to the node nearby approx. every ninth second. The time depends of the configuration. In a small system this could be every sixth second. Also this message is short - approx. 40 bytes plus the length of header (see item 2).

How do the messages look like e g for events and creating cardholders? What is size of packages is sent?

The packet size is currently 407 bytes (plus TCP header and IP header together with a MD5 hashing of the message). Totally it is less than 500 bytes. The information sent in case of an event (e g granted access) is approx. 40 bytes. Creating a new cardholder results in a database update with a frame of 80 bytes and a 10-byte frame.

How often does the SR35i communicate with each other?

At least every 6-8 second.

How often the SR35i does requests a timeserver?

It does it every 23rd hour continuously

What happens if the SR35i loses the database and uploads from another SR35i – does the LAN become slow?

No, because we only use a fraction of the total capacity. SiPass Entro uses 10/100 Mbit LAN and just a few percent of that. The reason is that the SiPass Entro primary should handle the access issues rapid. The communication has a lower task priority. In addition the communication is encrypted with 128-bit RC4, which together with the MD5 authentication takes CPU power and reduces the speed. However – in modern LANs switches are often used which not affect the speed negative.

Is it possible to change the IP port used by the system – e g if 4001 and 4002 are occupied by another application?

Only port 4002 is used in communication to the PC (and may be in conflict with other application is the same PC). You cannot change the port. The risk for a conflict is seen as minimal. If this should be a problem we will of course solve it. There are no applications known so far that uses this port.

How is the traffic affected? Use of “sniffers”?

We have (during the development phase) off course have been using “sniffers” (three commercial and one of our own). We have also bursted 100% bandwidth to

the SR35i to see the effects of the information quantity. Both UDP and TCP. This is however not quite so dramatic relative to a 100 Mbit LAN.

Why not use VLAN?

VLAN is a good alternative to create a more secure network. It is however difficult to state general recommendations how to build the users own LAN.

There is no reason for using VLAN, due to network load, in a SiPass Entro TCP/IP environment. In general we recommend IT-managers to use LAN switches rather than a SiPass Entro recommendation.

Can database files be placed on a LAN-server to make it possible making backups in night-time?

There are three main methods for central backups:

1. Each user modifies the path in the file dbpath.ini (on the local PC) to store the database files on his/her unique server folder (rather than in the local PC). You then must of course be sure that the server is running all the time. In this solution each user also connects to the SiPass Entro system.

2. Use SiPass Entro terminal server/client solution where both the files and the connection are done centrally.

3. If a Windows domain and a server-based profile storage is used the database is automatically stored to a server-share with every logout off the PC.

The way SiPass Entro is designed there is also redundancy integrated in the database, because all data is stored in every SR35i (except events handshaked from the PC).

Is the communication secure in Entro?

All communication in SiPass Entro is heavily encrypted. At the moment RSA RC4 128-bit is used. This is the same level as most banks are using. The encryption key can easily be changed. In Internet applications the IT-manager can raise the security by increasing the encryption set up in the LAN itself. In addition the User name and Password is checked at login as well as the correct System name.

What is RSA RC4?

RC4 is a symmetric encryption method, developed by RSA Security, which has been used for many years and is seen to be very reliable. SiPass Entro uses 128-bit strong encryption.

When comparing encryption algorithms, it is not correct to compare only the amount of bits because different encryption methods have different strength. SiPass Entro uses a symmetric method not to compare with e-mail software (usually using PGP or similar), which is an asymmetric method (with public keys). These methods normally require a higher size of key to fulfill the security need.

What is MD5?

MD5 is a method to confirm messages and logins. This is used in SiPass Entro to ensure that all messages are correct when they arrive. In addition also as an extra security when logging on via an web browser on to the Reservation system

28.2 What redundancy is there in the system?

The system is seen as very reliable. A breakdown often appears in the installation and set-up phase (or because of poor planning).

If there however is an accident, the SiPass Entro has a range of technical solutions that eases a fast trouble-shooting and repair. E g removable, straight-through terminal blocks support even a change of parts when the system is still running (somewhat like plug-and-play).

Under normal, preventive efforts we think that SiPass Entro (with its integrated monitoring functions and distributed intelligence) is very good alternative with good redundancy to reasonable price level.

Why use battery-backup (UPS)?

One of the best insurances against breakdowns etc. is to install the necessary amount of battery-backed power supplies. A correct planning regarding number of doors, type of locks, distances, cable type etc. is then of course a prerequisite.

We recommend every SR35i (together with its doors) to have its own power supply, if it is possible. First because of it gives a “cleaner” installation. Secondly it is possible to connect a power fail signal from the power supply to the system by using an IOR6. Every segment of the system can then separately be monitored for main voltage break-downs. An alarm event can be sent to the PC and/or an external alarm system (via IOR6).

What happens if a SR35i gets a short interruption?

Every SR35i as well as the PC have a complete copy of the database (mirroring). As long as the hardware is intact but an interruption occurs (e g the data memory is corrupt) the data is recovered automatically trough an up- or download. The stop of communication will generate an internal alarm to connected PC and/or an external alarm (via IOR6).

What happens if a SR35i fails?

Due the SR35i:s isolation capabilities the superior (global) communication will probably still work. If the door environment still has power and includes a DC22/DC12 (with memory) these will pass to an autonomic mode where decisions of access are taken locally. Other doors (without DC22/DC12) can be locked or unlocked. When the faulty SR35i is replaced it will automatically recover itself via a download from an-other SR35i (or PC). The event alarm functions still apply.

What happens if a reader or door controller fails?

In most cases other doors controlled by the same SR35i will still work. An alarm event will be sent from the actual SR35i if the door controller communication fails. When a reader fails this will be indicated in the System information window.

What happens during a cable failure?

A stop in the global communication (between SR35i Segment Controllers) will be discovered and an alarm event is sent from every SR35i respectively. The doors can work as normal.

A stop in the local communication (between a SR35i and door) will be discovered by the actual SR35i and an alarm event is sent from actual SR35i. The doors goes offline and some doors may also grant access dependent on the settings in the software.

A stop in the communication with the PC has the same effect as if the PC is turned off. I e all data is still stored in the system (together with an amount of events). Then the communication is established again and the PC goes on-line – all events are transferred automatically.

29 Important information form

Important information about the Access Control System

Regardless if any of the following information has been changed – the fields below should be filled in - and kept in a safe place. They will be needed if the system is to be changed in any way.

System name:

Encryption key 4 x 8 digits (0-9, A-F):

Password Installer program:

Name:
Password:

Password System User (Master):

Name:
Password:

Computers and connections

Name:	License number:	Connection:
		☐ TCP/IP ☐ RS232
		☐ TCP/IP ☐ RS232
		☐ TCP/IP ☐ RS232
		☐ TCP/IP ☐ RS232
		☐ TCP/IP ☐ RS232
		☐ TCP/IP ☐ RS232
		☐ TCP/IP ☐ RS232

30 Index

A

Access Control, 10
Alarm Status Feedback, 45, 98
Alarm zone, 97
Alarm Zones, 44
Anti-pass back, 42, 43, 100
AX, 70

B

BAPSI, 32
Bistable function, 98

C

Cancel time, 107
Card printing, 10
Card reader parameters, 81
CCTV, 10
CF8, 64, 120
Client, 25
Clock, 66
Common alarm, 93
Concurrent Reservations, 107
Confirmation, 113
Connection, 55, 117
Connections, 66
Crypto key, 115
CX, 72

D

Database, 24, 55, 117, 120
DC800, 121
debit, 111
Detection of units, 57
DHCP, 49, 87, 90
DNS, 49
Door controller, 91
Door Monitor, 10
Door monitor contact, 42
Door Monitor Contacts, 91
Download, 121
Duress, 82
DVR, 31, 65
DVR type, 66
Dynamic DNS, 49
DynDNS, 51, 52

E

E-mail, 111
E-Mail Server, 87
Emergency opening, 94
Entrance limitation, 101
Entro, 10
Entroser, 78
ENTRY reader, 43
ESD, 118
Ethernet, 25
EXIT reader, 43
Expansion, 115
external time server, 80

F

Factory crypto key, 115
Firewall, 52
Firmware, 120
Forward reservation time, 107

G

Gateway, 86
Grouped object, 105

H

HTML, 64

I

InfoPoint, 10, 29
Init string, 61
Installer, 10
Interlock, 102
Intrusion, 10, 44, 45
IOR6, 95
IP-address, 86

L

LED, 82
License, 24, 117, 118
License number, 58
Lift control, 95
Local power supply, 39

Lock monitor, 92
Lock monitor contacts, 91

M

MAC address, 50, 51
Machine control, 31
Memory card, 30
Modem, 59, 60
Multi-user, 58
MX, 68

N

Netmask, 86

O

Overlap time, 107

P

Password, 76
Patching, 120
Personal code, 81
Ports, 51, 66
Power failure, 94
Power supplies, 39
Power supply, 38
printer, 48

R

Readers, 119
Reservation, 10, 29
Reservation object, 104, 107
Router, 51
RS232, 48, 83
RS485, 25

S

Server, 25
SISTORE, 31, 65
SNTP, 80
SR34i, 116
SR35i, 83, 116
Static IP-addresses, 49
Subnet agent, 50

T

TCP/IP, 25, 83
Terminal Server 2008, 25
Termination resistor, 74

U

uninstall, 121
User name, 76

V,W

Wall socket, 48
Web server, 30
Viewer, 65
Wireless, 29
Voltage drop, 74

Issued by
Siemens Building Technologies
Fire & Security Products GmbH & Co. oHG
Siemensallee 84
D-76181 Karlsruhe
www.buildingtechnologies.siemens.com

© 2010 Copyright Siemens Switzerland Ltd
Technical specifications and availability subject to change without notice.

Document ID **A24205-A335-B317**
Edition 10.03.2010